Data form an increasingly essential element of contemporary politics, as both public and private actors extend claims of their legitimate control in diverse areas including health, security, and trade. This paper investigates data governance as a site of fundamental normative and political ordering processes that unfold in light of ever-increasing inter- and transnational linkages. Drawing on the concept of jurisdictional conflicts, the paper traces the evolution of data governance in three cases of transatlantic conflicts as diverging definitional claims over data. The paper argues that these conflicts reveal varying conceptualizations of data linked to four distinct visions of the social world. First, a conceptualization of data as an individual rights issue links human rights with the promotion of sovereignty to a vision of data governance as local liberalism. Second, proponents of a security partnership promote global security cooperation based on the conceptualization of data as a neutral instrument. Third, a conceptualization of data as an economic resource is linked to a vision of the digital economy that endorses progress and innovation with limited regulation. Fourth, a conceptualization of data as a collective resource links the values of universal rights and global rules to a vision of global protection.

La información constituye un elemento cada vez más esencial de la política contemporánea, ya que tanto los actores públicos como los privados reclaman el control legítimo de esta en diversas áreas, incluida la salud, la seguridad y el comercio. En este artículo, se investiga la gestión de la información como un lugar de procesos de ordenamiento normativos y políticos fundamentales que se desarrollan a la luz de los crecientes vínculos internacionales y transnacionales. A partir del concepto de conflictos jurisdiccionales, este artículo traza la evolución de la gestión de la información en tres casos de conflictos transatlánticos como reclamos de definición divergentes sobre la información. El artículo sostiene que estos conflictos revelan diferentes conceptualizaciones de la información vinculadas a cuatro visiones distintas del mundo social. Primero, la conceptualización de la información como una cuestión de derechos individuales vincula los derechos humanos con la promoción de la soberanía a una visión de la gestión de la información como liberalismo local. Segundo, los defensores de una asociación de seguridad promueven la cooperación mundial en materia de seguridad basándose en la conceptualización de la información como un instrumento neutral. Tercero, la conceptualización de la información como recurso económico está vinculada a una visión de la economía digital que respalda el progreso y la innovación con una regulación limitada. Cuarto, la conceptualización de la información como un recurso colectivo vincula los valores de los derechos universales y las normas mundiales a una visión de protección global.

Les données constituent un élément de plus en plus essentiel des politiques contemporaines car les acteurs publics et privés étendent tous deux leurs revendications de contrôle légitime dans divers domaines, notamment dans ceux de la santé, de la sécurité et du commerce. Cet article enquête sur la gouvernance des données en tant que site des processus fondamentaux d’organisation normative et politique qui se déploient au vu des liaisons internationales et transnationales qui ne cessent de se développer. S’appuyant sur le concept de conflits juridictionnels, cet article retrace l’évolution de la gouvernance des données dans trois cas de conflits transatlantiques prenant la forme de revendications définitionnelles divergentes sur les données. Il soutient que ces conflits révèlent des conceptualisations variables des données qui sont associées à quatre visions distinctes du monde social. Premièrement, une conceptualisation des données en tant que question de droits individuels associe les droits de l’homme et la promotion de la souveraineté à une vision de la gouvernance des données en tant que liberalism local. Deuxièmement, les partisans d’un partenariat de sécurité promeuvent une coopération internationale de sécurité reposant sur la conceptualisation des données en tant qu’instrument neutre. Troisièmement, une conceptualisation des données en tant que ressource économique est associée à une vision de l’économie numérique qui soutient le progrès et l’innovation avec une réglementation limitée. Quatrièmement, une conceptualisation des données en tant que ressource collective associe les valeurs des droits universels et des règles mondiales à une vision de protection internationale.

Introduction

The ever-increasing relevance of the internet has contributed to the recognition of data as a key concern in social, political, and economic lives. How data are collected, processed, and shared has significant implications for contemporary politics in areas, such as security, health, democracy, and human rights (van Puyvelde, Coulthart, and Hossain 2017; Davies and Wenham 2020). After the 2013 Snowden revelations of mass surveillance by intelligence agencies around the world but also following potential voter manipulation in the Cambridge Analytica scandal in 2018, data governance has experienced a “salience shock” (Kalyanpur and Newman 2019). Data governance describes ordering processes by actors including but not limited to states, international organizations, local authorities, and private companies that relate to the processing, transfer, sharing, and general use practices of digital data. Regulatory measures...
on the international, regional, and domestic level have proliferated. Of the 132 countries that have at least minimal data privacy laws in place, 55 countries have adopted such legislation only in the last ten years (UNCTAD 2020). As even tech companies have increasingly called for regulation (Hern 2019), former European Commissioner Marine Reicherts has claimed that “[d]ata protection is the new business model” (Reicherts 2014). While there seems to be convergence around common standards (Bradford 2020), conflicts resulting from different approaches to the governance of digital data have shaken particularly transatlantic relations in the last decade (Farrell and Newman 2019). Actors face significant incentives to avoid such conflicts. In 2013, the European Centre for Political Economy estimated that a serious disruption in transatlantic data flows could have a negative impact on the EU Gross Domestic Product of between 0.8 and 1.3 percent (ECIPE 2013, 3). Yet, overlapping claims of control have adversely affected the transatlantic data transfer regime multiple times. For instance, in 2015 and again in 2020, the Court of Justice of the European Union (CJEU) invalidated the main transatlantic data sharing agreement for commercial transfers exposing more than 5,000 businesses to legal uncertainty.

How can we understand the prevalence of conflicts despite these significant consequences? This paper sets out to disentangle the diverging trajectories of convergence and conflict in transnational data governance. Existing approaches in the literature have foregrounded the legal or institutional dimensions of contestations. On the one hand, a substantial branch of legal scholarship illustrates the difficulties that emerge from distinct legal approaches and problematizes the extraterritorial reach of regulatory measures (Reidenberg 2000; Bignami and Resta 2015; Kuner 2015). Yet, it neglects the political negotiation processes that resolve these differences. On the other hand, scholars in International Relations (IR) and International Political Economy have outlined how institutional conditions and power dynamics shape the emergence and resolution of contestations (e.g., Bennett and Raab 2006; Schümann and Baumann 2017; Farrell and Newman 2019; Fahey and Terpan 2021; Ripoll Servent and MacKenzie 2011). However, except for a branch of literature in critical security studies (Amoore and Raley 2017; de Goede 2018), these approaches fail to problematize the notion of data as a fixed object.

This paper suggests that diverging constructions of data governance are a so-far underestimated and undertheorized factor in current governance controversies. Actors conceptualize differently the meaning of data, the relevant stakeholder community, and the reasoning for their governance efforts. I argue that these elements represent distinct visions, or socially constructed realities, of data governance. The paper selectively draws on relational sociological theory to analyze these conflicts through the framework of “jurisdictional conflicts” (Abbott 1986). This approach illuminates how actors articulate overlapping claims over an issue based on a system of knowledge or control (Abbott 1988, 8). Thereby, they engage in a process that is co-constitutive with the very object they are attempting to govern. The paper suggests that while actors seem to resolve their overlapping claims over data, diverging regulatory responses persist due a lack of shared understanding of data as a governable object and the goals of data governance per se. This paper illustrates the relevance of such conceptualizations in three exemplary cases of conflict that have emerged at the interface of such overlapping claims: first, the dispute about transatlantic commercial data transfers after the Snowden revelations, second, the conflict around electronic evidence between Microsoft and the US Department of Justice (DoJ), and, third, the conflict between the European data protection authorities and Google regarding the potential global applicability of the right to be forgotten. These diverse issue areas include moments of intense debate that clearly articulate underlying differences but at the same time demonstrate how controversies are temporarily stabilized.

The paper makes a conceptual argument by highlighting that governance objects are not only related to expertise and knowledge. Instead, it systematically assesses the normative impetus behind justificatory practices that create such objects. More specifically, I suggest four conceptualizations of data as a governable object that are embedded in and entangled with distinct ideas about the right conduct of governance. These visions of data governance describe what data governance is about, what it should achieve, and what justifications are considered acceptable. First, those conceptualizing data as an individual rights issue link human rights with the promotion of sovereignty to a vision of data governance based on local liberal protection. Second, proponents of a security partnership promote global security cooperation and conceptualize data as a security tool. Third, a conceptualization of data as an economic resource is linked to a vision of the digital economy that endorses progress and innovation but limited regulation. Fourth, the idea of data as a collective resource emphasizes universal rights and global measures.

The paper makes three contributions. First, by illuminating the constitution processes of data as a governance object, the paper contributes to a shift from a focus on “subjects to objects” (Allan 2017, 842) in IR scholarship. At the same time, it answers calls for a more conceptual debate on (big) data in various governance sectors (see e.g., van Puyvelde, Coulthart, and Hossain 2017). The paper fills a gap in the literature by bringing interdisciplinary insights concerning the conceptualization of data to debates in international studies and expands the existing insights beyond the context of security practices (Amoore and Raley 2017; de Goede 2018). Second, the paper captures these insights through comprehensive and distinct visions of data governance. This links the literature on the constitution of objects (e.g., Sending 2015) to a growing recognition of the normative quality of policy standards and regulation (Kjaer and Vetterlein 2018). On the one hand, it points to the importance of normative ideas in transnational governance. On the other hand, it highlights the comparatively stable nature of conflicts over meaning in a context that tends to be characterized in terms of its fast pace. Third, by drawing on a sociological understanding of “jurisdictional conflicts,” the paper emphasizes that jurisdictional claims are neither only technical, legal, or power claims but encompass a specific normative vision of the social world. While the normative character of data governance creates space for disruption even by marginalized actors, entrenched structures often prevent change in the long term.

The paper is structured as follows: In the next section, I will first outline the theoretical framework of jurisdictional claims to specify object construction processes around the conceptualization of data. Second, outline the chosen methodological approach of a discourse analytical reading of policy documents and my coding process. Third, I will briefly describe the identified visions of the social world based on distinct conceptualizations of data as a governable object, the reference community, and the underlying justifications before moving to three illustrative cases in a fourth step. These cases show the specific struggles between actors and normative principles in data governance. I will compare these examples in a fifth step before, in the final part of the
paper, I conclude with a brief outlook of potential future developments and further research.

**Overlapping Jurisdictional Claims in Data Governance**

Data are difficult to regulate, particularly on a transnational level. The ordering and steering processes of data governance cut across multiple issue areas and actors. The lack of a central international authority and the fast pace of technological development often results in the absence of clear rules of conduct. Governance challenges are exacerbated by two intersecting dynamics: On the one hand, the prevalence of extraterritorial consequences of regulation contributes to overlap between local and global claims of control. On the other hand, the central position of particularly private tech companies produces a complex web of public and private claims. These claims frequently feature clashing regulatory demands. The lack of institutional mechanisms at the global level means that there are rarely straightforward ways of resolving such conflicts of overlapping jurisdiction (Buxbaum 2009; Efrat and Newman 2016). Therefore, frequent conflicts have been a characteristic of data governance in recent years. They are relevant because their resolution shapes the relationship between the state, companies, and individuals by determining their rights and obligations.

The understanding of jurisdictional conflicts has been shaped primarily by legal scholars (Mitsilegas 2014; Kuner 2015; Ryngaert 2015) and by some political scientists (Efrat and Newman 2016). Both have highlighted the need to move beyond territorial conceptions of jurisdiction, for example specifying the need to incorporate practices of deference (Efrat and Newman 2016) or introducing the notion of community (Ryngaert 2015). I adopt a sociological understanding of jurisdiction and draw on a relational approach developed by Abbott (1986). Relationalism investigates the relations between actors or objects and the processes that stabilize and mutually construct them (McCourt 2016, 479). By emphasizing the historicity of such relations, this approach pays attention to the processes that enable the constitution of the specific object of study, in our case data. Adopting such a relational approach to jurisdiction emphasizes how the negotiation processes constitute relations between objects and actors. Jurisdiction is not only understood as a legal or territorial domain but also in an epistemic sense. By issuing “jurisdictional claims” (Abbott 1986, 191), actors establish their jurisdiction as a sphere of competence, defined as “legitimate control over an issue” (Abbott 1986, 191). I distinguish between three elements of a jurisdictional claim. Through their claim of legitimate control over data actors define:

1. the *object of governance*, that is, what they are attempting to control;
2. their *reference community*, that is, their actorness in relation to the affected stakeholders;
3. the *justification*, that is, why their claim is legitimate.

By issuing a claim over a specific issue in the name of a specific community for specific reasons, actors demarcate acceptable and unacceptable policy responses. Together, these form *regulatory visions* of data governance. In jurisdictional claims, actors draw on these visions as justificatory bases and, at the same time, construct and refine them. When overlapping claims clash, “jurisdictional conflicts” (Abbott 1986) arise. How do they unfold?

First, when actors articulate overlapping claims over an issue based on a system of knowledge or control (Abbott 1988, 8), they co-constitute the very object they are attempting to govern. For instance, when actors simultaneously claim control over data to specify where and to whom data belong and why they should be governed, they constitute data as a governable object with specific characteristics. If data governance emphasizes the free flow of data for commercial purposes, this is incompatible with an understanding of data intimately linked to individual dignity. To conceptualize this process, I draw on an emerging branch of literature in IR and its roots in sociology that focus on how technologies are “discursively ‘formed as objects’” (Boettcher 2020, 7) and how this shapes their governance. Particularly current research on the creation of knowledge through science, expertise, and professionals (e.g., Sending 2015; Allan 2017; Hanrieder 2019) explores how individuals and communities relate to the constructed meanings of objects.

This perspective contributes to existing work on data governance in media studies, critical security studies, as well as interdisciplinary research. Here, scholars have investigated the ideological roots of datafication (van Dijck 2014), the genesis of data as a constructed concept (Gitelmans 2013), and data-based value judgments through algorithms (Gillespie 2016; Amoore 2020), particularly in the context of “algorithmic regulation” (Yeung 2018). Algorithmic regulation denotes a form of social ordering based on big data and statistical methods that is associated with particular normative commitments. Drawing on this literature, Bellanova and de Goede (2020) as well as Ulbricht (2018) have outlined how the technological choices and infrastructural settings in the collection of air travel passenger and financial data significantly impact the regulatory process. In the broader context of security and counterterrorism, scholars including Aradau (2020) and de Goede (2018) have described the transformation of data from mundane data fragments into mystical and simultaneously depoliticized (security) facts. Particularly in intelligence and counterterrorist contexts, data are turned into a neutral and depoliticized “tool” available for use in the pursuit of suspects.

Second, the definition of a specific object, issue, or duty of governance not only co-constitutes a governance object but also represents a claim to act on behalf of others (Abbott 2005). In the case of data governance, actors implicitly or explicitly construct a reference community of stakeholders—those affected by the (lack of) control over data collection and processing. This implicit or explicit construction of such a reference community provides legitimacy to some claims, actors, and actions rather than others (Sending 2015, 28).\(^1\) The conceptualization of governability of data in a specific way, such as global or local, public or private, similarly has implications for whose claim may be considered legitimate. For instance, Allan (2017) has highlighted how the specific constitution of “the climate” as an epistemic object established the legitimacy of new governance subjects, such as expert bodies, that conform to the characteristics inscribed into the object of governance. The literature on epistemic practices frequently focuses on professions or experts (Knorr-Cetina 1999; Hanrieder 2019), but these groups are more fluid in data governance. While, for example, data protection professionals have shaped the development of legislative frameworks particularly in the beginning, they by no means hold a dominant role in data governance, neither epistemically nor in regulatory functions (Raab and Szekely 2017).

\(^1\) Similar struggles have been described as a competition over epistemic authority among diverse actors such as states, non-governmental organizations (NGOs), and groups of policymakers (Sending 2015; Stroup and Wong 2017).
Abbott further highlights that dominant control both in and through jurisdictional conflicts is rare, foregrounding the analysis of “how jurisdictions are opened, contested, and closed” (Abbott 1986, 192). This procedural emphasis also recognizes the fragile nature of even institutionalized agreements. Fauche and Große-Kreul (2020) have argued that institutional overlap may enable actors that are marginalized within one institution to demand justification via inter-institutional justificatory practices. Thus, actors may be similarly likely to draw strategically on conceptions brought forward in other jurisdictions to demand justifications and challenge the status quo. Institutional frameworks, such as the Privacy Shield that governed transatlantic commercial data flows until its invalidation in July 2020 (Fahey and Terpan 2021), often fail to resolve the underlying differences in the conceptualizations of data as governable objects and the broader social ideas behind them. While some actors may temporarily stabilize their claim sufficiently to impose an institutional solution, they fail to fix the meaning of data.

Third, jurisdictions exemplify distinct normative approaches to regulation (Johns and Compton 2019), which provide legitimacy to specific actors by determining the moral worthiness of practices and specific forms of evidence. The literature on data governance tends to overlook or simplify the foundational normative character of current controversies. For example, Ruppert, Isin, and Bigo (2017) investigate the interrelations between data as a constructed object of knowledge and an object of power but do not explicitly examine the normative impetus behind such constructions. While the literature has highlighted that data governance is shaped by the conflicting goals of “freedom” versus “security” (e.g., Farrell and Newman 2019), including through securitization (Balzacq 2007), these goals are too narrow and, at the same time, not fully specified. It is therefore imperative to recognize the normative plurality of such claims. Regulatory efforts require justifications that correspond to the specific normative context in which they are embedded (Kjaer and Vetterlein 2018, 500). Therefore, jurisdictional claims reach beyond professional expert claims by bringing forward actors’ (clashing) moral convictions. To justify their claims, actors link their claim to higher universal principles (Boltanski and Thévenot 2006). They articulate broad ideas about what is morally worthy and unworthy behavior. I suggest that by formulating jurisdictional claims, actors mobilize and at the same time generate distinct visions of data governance. They articulate deep normative ideas that outline what data are and how they should be governed, for and with whom, and why. The visions denote how actors combine those ideas into more comprehensive worlds of data governance.

In sum, the existing literature tends to neglect the multidimensional nature of conflicts as political, legal, institutional, and normative struggles among public and private actors about the right conduct of data governance. I argue that the understanding of jurisdictional claims including the three elements of object of governance, reference community, and justification helps grasp this multidimensional nature of conflicts. These jurisdictional claims have a co-constitutive relationship with distinct visions of data governance. This paper presents a typology of these visions derived inductively from the empirical analysis. I suggest that these visions compete and remain stable throughout different controversies, across issue areas, and over time.

The previous section outlined the understanding of conflicts in data governance as jurisdictional conflicts that emerge at the intersection of distinct regulatory visions. In this section, I will outline my methodological approach in researching those visions.

In the articulation of jurisdictional claims, that is, claims of legitimate control over a certain issue, actors draw on and create distinct social realities or visions. The paper follows an interpretivist approach, emphasizing the constructed nature of social relations through practices and processes of meaning making. I suggest that jurisdictional conflicts represent moments of uncertainty during which actors need to articulate their claims in reference to broader principles (Boltanski and Thévenot 2006). Yet, these discursive practices do not happen in a power vacuum. This highlights tensions between taking the normative and moral aspects of such claims seriously while not ignoring the exercise of power inherent in such practices of meaning making in discourse. In following calls for theoretical cross-fertilization (Leipold et al. 2019), this paper is inspired by an understanding of discourse that focuses on the sociology of knowledge. This approach forefronts “[e]vents, problematisations and their actors who are engaged in the politics of knowledge and knowing, that is, in meaning/world making” (Keller 2018, 17). It highlights how objects are constructed as governable and therefore linked to the demarcation of adequate and inadequate policy problems and decisions.

The paper reconstructs the politics of such meaning-making processes in the unfolding of conflicts over time in three cases. The cases exemplify jurisdictional conflicts as a specific empirical phenomenon in data governance (Gerring 2004, 342). They cover the transatlantic context, which comprises currently the most impactful regulatory battles and key actors in data governance. Both in regulation and norms, data governance has been heavily shaped by processes of meaning making resulting from the interaction of EU institutions, the United States, and private companies (Farrell and Newman 2019). I included cases with at least one formal legal jurisdictional claim to illustrate the relevance of a sociological perspective also in seemingly narrow legal cases. Therefore, the number of potential cases is comparatively small. Two additional cases of transatlantic jurisdictional conflict over data in counterterrorism regarding air travel and finance are substantively better covered in international studies (e.g., Bellanova and de Goede 2020; Ripoll Servent and MacKenzie 2011). The paper extends these insights about data-related processes of meaning making to policy domains beyond security and counterterrorism. While this necessarily limits the detail provided by each case and particularly shortens the reflections on the internal tensions and contestations of actors such as the United States, the comparative approach of the paper outlines how such processes of construction play out in different settings.

To illustrate differences between actors’ realities, I examined the claims of control that actors issued either implicitly (e.g., by introducing a specific legislative act or in issuing a formal data request) or explicitly (e.g., in court submissions). Using the software MAXQDA, I coded statements according to the three elements of a jurisdictional claim derived from the theoretical literature: (a) conceptions of data as the object of governance, (b) the reference community, and (c) underlying justifications. Within these categories, I relied mostly on inductive coding and adapted the coding...
scheme through multiple iterations. I coded these elements according to content rather than formal structure, so a single coding unit could comprise part of a sentence or a paragraph if it represented at least one of the three elements of the jurisdictional claim. I allowed overlapping codings of the same claim if it referred to multiple conceptions or justifications.

The analysis draws on a variety of primary sources, including policy and legal as well as leaked text documents, such as court proceedings and submissions, press releases, and company blog entries. I selected documents from all parties involved in the conflict until saturation was reached, that is, when the identified categories, perspectives, and codes covered all new material. In total, I coded ninety-nine documents. The different types of documents are representative of the distinct ways through which actors express their jurisdictional claims. The inclusion of a wide range of documents for the same categories increases the possibility to grasp the evaluative repertoires of different actors.

In addition, I conducted twenty-one semi-structured, problem-centered qualitative interviews with representatives from the public and private sector between December 2017 and November 2019.4 Interviews took place at policy conferences, such as the Internet Governance Forum, and with policy-makers in Brussels and Washington, D.C., and with company representatives in Silicon Valley. Interviewees were selected based on snowballing to cover a variety of perspectives from the involved conflict parties. The interviews mainly provided background knowledge to triangulate information and added insights about existing visions of data governance.

Based on the clustering of codings, I provide an empirically grounded and inductively developed typology of four visions of data governance. This represents a synthesis of the findings of how these codes manifested and co-occurred in the empirical cases. I grouped codes through iterative processes to arrive at visions that grasped most justifications. I will outline these visions in the next section.

### Competing Conceptualizations of Data Governance

As outlined earlier, the increased salience of data governance has not resulted in agreement about the meaning of data and the justification for regulation. Indeed, there are divergent ideas that relate to the elements of governance object, reference community, and justifications. Together, these elements form four distinct visions of data governance that feature underlying conceptualizations of data, including data as an individual rights issue, an economic resource, a security tool, or a collective resource (see Table 1). These conceptualizations describe assumed key characteristics of data and correspond to the pursuit of collective values, that is, individual fundamental rights, economic progress and innovation, security and safety, and universal rights and goods. In addition to these substantive goals, there are differences that pertain to certain reference communities of a more local or global and more private or public character, respectively.

First, I suggest that actors follow an idea of local liberalism in data governance, characterized by a local outlook that emphasizes the common good of human and fundamental rights of individuals, including principles such as equality, justice, and necessity. It highlights a fundamental rights-based conceptualization of data. In this vision, data are irrevocably tied to the individual and may be used only under circumstances that respect individual rights and potential implications for human dignity. This vision is based on justifications of justice and fairness, as well as cultural and political articulations of liberal values. In addition, this vision is also characterized by an emphasis on public authority and strong, enforceable norms and rules as well as by justifications linked to sovereignty.

Second, an opposing vision I term digital economy is based on a specific combination of references to individual rights, economic progress, and global solutions, which focuses on the importance of data as an economic resource. Data are constructed as a valuable resource that needs loose and interoperable regulation to be effectively distributed for profit. Rather than focusing on its relevance for the individual, however, this notion of data is comparable to Zuboff’s notion of “raw material” (2018, 8) that can be processed and monetized. The vision emphasizes principles such as trust to strengthen the customer’s relationship with the digital economy and highlights the importance of innovation, freedom of enterprise, and legal certainty for companies.

Third, I observe a shift toward looser global structures in security-related areas in the field of data governance that represents the vision of a security community. This vision conceptualizes data as a security tool, which highlights how, for example, in air travel or law enforcement, data are conceptualized as a neutral instrument in the fight against terrorism or crime. The idea of a tool reflects the implicit assumption that (background) knowledge is necessary to work with data, highlighting the transformation of mundane data into classified information (see also De Goede 2018) as part of the jurisdictional claim of security professionals. This vision is based on global security threats that require global cooperation and common solutions to provide safety. Data are necessary in the fight against impunity, a challenge exacerbated by the internet and transnational crime and terrorism. Through incremental processes that establish security

---

4See online Appendix for list of interviews. Personal information has been retracted according to the interviewees’ preferences.
and safety as the ultimate goals of data governance, often enabled by the convergence of public and private interests, an existentially threatened community is created.

Fourth, a vision of global protection emphasizes interoperable standards in data governance. In this vision, data are conceptualized as a collective rather than an individual rights concern. Data are valued as a common resource and required common solutions for effective use. Their collective character also demands universal access. Therefore, regulation demands stronger cooperation and legal harmonization to avoid fragmentation and international discord. This vision emphasizes principles such as solidarity and universalism, highlighting the importance of interoperable standards.

In summary, the four visions of data governance suggest what data are, who should govern them, and why data governance is meaningful. The next section outlines how these visions manifest empirically in and through jurisdictional claims.

Results: Struggles in Global Data Governance

After outlining the theoretical and methodological approach and presenting four distinct visions of data governance, this section will analyze three manifestations of ongoing struggles between these visions. I focus on the resources that actors employ in and through object construction processes as well as the broader visions of data governance. This approach highlights the co-constitutive relationship between instances of conflict and the conceptualization of data as a governable object. For each contested area, I will summarize the initial contestations, responses, and outcomes before briefly pointing to broader implications for the field. While the outcomes of negotiation processes tend to produce tangible institutional measures, such as bilateral agreements or legislation, the resulting jurisdictional configurations are often fragile and subject to challenges in the future.

Transatlantic Commercial Data Governance

In this first exemplary case, I focus on the clashing jurisdictional claims of US intelligence surveillance and the EU’s data protection regime. The 1995 EU Data Protection Directive, like its successor, the 2016 General Data Protection Regulation, constitutes a jurisdictional claim of control over EU data. These legislations heavily restrict data transfers to jurisdictions outside the EU. Only if the European Commission finds the jurisdiction’s standards of data protection to be adequate, data may be transferred. This is not the case for the United States. In turn, through its comprehensive surveillance activities, US intelligence services issued an overlapping claim of control over EU data.

In 2000, the United States and the EU attempted to bridge their regulatory differences through the so-called Safe Harbor agreement. The self-regulatory framework allowed US companies and organizations to meet the requirements of the 1995 Data Protection Directive and transfer data with adequate protection. Despite criticism, the agreement remained largely unchallenged until high issue salience after the revelations of NSA mass surveillance by US whistle-blower Edward Snowden put pressure on EU institutions to enhance legitimacy (Kalyanpur and Newman 2019). While negotiations for a potential reform of the framework were still ongoing, Maximilian Schrems, an Austrian citizen, filed a complaint about the lack of adequate data protection concerning the US-based company Facebook. This complaint became the subject matter of a court case eventually referred to the CJEU. After fifteen years of rather unobtrusive existence, the transatlantic framework for commercial data sharing suddenly was at the center of attention when the CJEU invalidated the agreement. Despite significant protests by the United States, the negotiation of a new agreement became necessary.

Making the Object of Governance

The extraterritorial nature of the surveillance measures by the NSA developed into a significant source of conflict in EU–US relations, particularly regarding sovereignty concerns. In 2013, the European Commission conducted a Safe Harbor framework review that largely focused on the economic implications. The Commission identified Safe Harbor as “one of the conduits through which access is given to US intelligence authorities” (EC 2013, 16) but mainly focused on potential damages resulting from broken trust and suggested any change could be “adversely affecting the interests of member companies” (EC 2013, 7). Rather than a human rights or security concern, the Commission publications conceptualized data as a valuable economic resource, which needed to flow freely between the two jurisdictions, and particularly a reference community of affected companies.

Schrems’ complaint challenged this perspective in reference to a rights-based account of data. Due to the significant reliance of the NSA on cooperation with private service providers, the data collection and transfer practices could be considered as commercial and therefore protected by EU law. This provided a possibility to contest the legal basis for both types of data use based on the protection of EU citizens by law (Schrems 2013). This conceptualization thus emphasized liberal goals of protecting individual rights in a reference community of EU citizens.

Statements by US actors did not address the Safe Harbor framework specifically. Instead, announcements were restricted to general security references. For instance, President Obama argued “[b]ut I think it’s important to recognize that you can’t have 100 percent security and also then have 100 percent privacy and zero inconvenience. We’re going to have to make some choices as a society” (Obama 2013). Facebook took a similarly passive stance and explicitly argued that “this case is not about Facebook” (Price 2015), deferring authority to public actors. While US actors vaguely attempted to link data governance to security justifications, they failed to assert their jurisdictional claims. Thus, the dominant conceptualizations of data juxtaposed an economic resource with a fundamental rights concern.

Responses and Justifications

Based on the conceptualization of data governance as primarily economic in character, the Commission prioritized “strengthening” (EC 2013, 7) the existing Safe Harbor over negotiating a new framework. The CJEU case enforced clear assessments of the compatibility of NSA surveillance and the EU legal framework. The European Parliament (EP) called for an immediate suspension of the framework in 2014 referring to human rights (EP 2014, 40). However, none of the actors in the EU was willing to argue that US bulk surveillance practices constituted a necessary derogation in line with the agreement, as this was not perceived as politically feasible (EC official, 2019, personal interview). This implicitly entrenched data as a rights-based concern with implications for sovereignty, strengthening the vision of liberal protection.
While it is difficult to estimate the consequences of a potential US involvement in the discourse, the US government has been considerably more active in subsequent court proceedings (Moody 2016). The lack of engagement was likely based on a misrecognition of the US’s own position of power, which failed to sustain the US claim. In contrast, the Parliament and Schrems proactively attempted to shape the meaning making process, emphasizing the “indiscriminate practices of mass surveillance” (EP 2014, para. K). This suggested that the US’s jurisdictional claims violated a rights-based vision of data governance. In consequence, the CJEU based its assessment of US surveillance laws and practices on these dominant conceptualizations.

OUTCOME
Since the European Commission in its definition of adequacy in 2000 had failed to assess the broader legal framework in the United States, the CJEU declared its adequacy finding invalid. This also invalidated the Safe Harbor framework (CJEU 2015). While most US actors seemed surprised by the ruling highlighting misunderstandings and stated they were “deeply disappointed” (Pritzker 2015), one interviewee from the Commission described that it “felt like we saw the train coming towards us and could do nothing to avoid the crash” (EC official, 2019, personal interview). Despite the immense material interests behind commercial transatlantic data transfers, the regime was suspended. Rather than establishing NSA surveillance as a necessary answer to an existential threat in the pursuit of security, data were conceptualized as an individual rights issue with implications for communal integrity.

The judgment had eliminated most options for incremental change, it even strengthened the position of the EU in the global arena. The Commission, through the sense of urgency that followed the CJEU decision, was able to both enlarge and constrain the space of policy options vis-à-vis the United States and the other EU actors. The EU was able to push for stronger safeguards, which in turn set new standards for the protection from public surveillance practices in the field. In February 2016, renewed negotiations culminated in the EU-US Privacy Shield agreement, which replaced the Safe Harbor framework. In July 2020, however, the CJEU again struck down the Privacy Shield agreement, based on insufficient safeguards and the ineffectiveness of oversight in relation to US intelligence services (CJEU 2020). The judgment’s effects are still unclear, as both regulators and the Commission negotiators seem to be struggling to find a solution to a problem that essentially demands a profound change of intelligence practices.

In conclusion, despite significant power imbalances, Schrems’ complaint established the US jurisdictional claims as inadequate based on a rights-based conceptualization of data emphasizing individual integrity. This converged with the preferences of other actors to uphold sovereignty and protect EU citizens as a reference community. This resulted, twice, in the invalidation of a central bilateral agreement as well as a narrower legal conceptualization of adequate protection of data in the EU. This emphasis on the fundamental rights character of data also resulted in the recent invalidation of Privacy Shield, which had failed to strictly constrain surveillance practices.

Electronic Evidence
In this second exemplary case, a jurisdictional conflict emerged over access to electronic evidence. The company Microsoft, the United States, and Europe all draw on different resources to sustain their jurisdictional claims over data in law enforcement investigations. As the extent of online interactions is increasing, the significance of electronic evidence for law enforcement is on the rise. This includes, for example, email correspondence, conversation metadata or IP addresses linked to criminal activities. To avoid the highly formalized Mutual Legal Assistance Treaty (MLAT) procedures to gain access to these data, which takes an average time of 6–9 months, law enforcement agencies have increasingly relied on direct informal cooperation with internet service providers (Europol 2019). While entirely voluntary, these requests constitute jurisdictional claims by law enforcement officers. This has left significant legal uncertainty for the companies involved, because they have to assess the legitimacy of the requests. In 2013, Microsoft used its key position as the holder of large amounts of data to challenge the status quo by resisting a warrant issued by the US DoJ. This designated the jurisdictional claim as illegitimate. The warrant requested content data that were stored in Ireland. Microsoft argued that the referenced 1986 US Stored Communications Act did not authorize extraterritorial data access. Instead, Microsoft suggested that the data were subject to jurisdictional claims by EU data protection law that prohibited onward transfers, referring to a local liberal vision of data governance. Other companies quickly joined and thus enforced public justifications for this relatively unknown practice of law enforcement agencies (Tech company employee, 2019, personal interview). In 2017, the case reached the US Supreme Court (2018), which reinforced public attention to the global relevance of this jurisdictional conflict. In March 2018, the case became moot, when the US adopted the Clarifying Lawful Overseas Use of Data Act (2018), a law explicitly legalizing data access under particular conditions (see Daskal 2018).

MAKING THE OBJECT OF GOVERNANCE
During the conflict, actors brought forward a variety of conceptions of data and corresponding notions of stakeholder responsibility. Microsoft attempted to define the criterion of evaluation by highlighting a violation of privacy standards (Smith 2018a) thereby illegitimizing the jurisdictional claim from the United States. While this conceptualization of data as an individual rights concern contributed to issue salience in public discourse, it found only limited acceptance among the conflict parties. The US DoJ emphasized security as the relevant goal of data governance. This conceptualized data as evidence:

“[…] hundreds if not thousands of investigations of crimes — ranging from terrorism, to child pornography, to fraud — are being or will be hampered by the government’s inability to obtain electronic evidence. […] The decision protects only criminals whose communications are placed out of reach of law enforcement officials because of the business decisions of private providers.” (US 2017, 128)

This reference to an existential threat foregrounded the goal of security by highlighting the problematic consequences of ignoring a security-based conceptualization of data. In contrast, Microsoft increasingly conceptualized data as akin to a physical object. For example, a Microsoft representative argued that “[t]he government wants to use the act to unilaterally reach into a foreign land to search for, copy, and import private customer correspondence physically stored in a digital lockbox, any foreign computer where it’s protected by foreign law” (Supreme Court of the US 2018, 52). These references entrenched the nature of data
requests as violent and intrusive and pointed to a potential violation of sovereign integrity.

The conceptualization of data also included references to specific communities to support the jurisdictional claims of some actors rather than others. For instance, the US representative Dreeben attempted to delegitimize Microsoft’s claim pointing out that “Microsoft is basically claiming the authority, once it moves the information overseas, to unilaterally disclose it to anyone” (Supreme Court of the US 2018, 67). This established a hierarchical relationship between legitimate public and irresponsible private actors. In turn, Microsoft juxtaposed US sovereignty-intruding practices with its own responsible behavior to legitimize its political action (Supreme Court of the US 2018, 60). While the conceptualization of data as a sovereignty concern was recognized, both the US efforts of establishing data access as a necessity for security cooperation as well as Microsoft’s privacy justifications were largely ignored.

Responses and Justifications

While the legal case initially had a largely domestic character, the implications for sovereignty contributed to an increasing relevance for other jurisdictions. This added a public/public dimension to the previously public/private nature of the jurisdictional claims. Various actors submitted amicus curiae briefs to the Supreme Court, including the European Commission, Ireland, several NGOs, and the UN Special Rapporteur for Privacy Online. The fact that international actors became involved in a domestic court case was perceived as striking (Supreme Court of the US 2018, 13) and further entrenched data governance as a matter of sovereignty (EC 2018a, 14).

The general hesitance of the Supreme Court to resolve the jurisdictional conflict as well as the threat of potentially damaging legal precedence catalyzed a legislative process in the United States. The resulting CLOUD Act (2018) specified conditions for legal data access for law enforcement agencies and thus supplemented the jurisdictional claim through legislation. Adopted while the case was still in court, the bill evaded a more comprehensive debate in Congress when it was passed on page 2212 of a 2232-page omnibus spending bill that was required to avert a government shutdown. Despite the persistence and even reinforcement of extraterritorial effects, the CLOUD Act was met with surprisingly little public resistance from the EU. Microsoft similarly referred to the CLOUD Act as an “important milestone” (Smith 2018a), which strengthened and legitimized the jurisdictional claims by public actors.

Outcome

The CLOUD Act did not resolve the underlying differences in conceptualization of data and data-related sovereignty intrusions. Considering the persisting jurisdictional conflict, the acceptance might seem surprising. Yet, only two months later, the Commission published its own two-fold legislative proposal to regulate electronic evidence sharing, which also emphasized the practice as an important means to “counter modern forms of criminality” (EC 2018b, 2). The Commission also “move[d] away from data location as a determining connecting factor” (EC 2018b, 13), thus abandoning the sovereignty-based conceptualization of data. In addition, comparable regulatory initiatives in the Council of Europe have highlighted the importance of international cooperation (CoE 2018). The provisions in both proposals are in many ways similar to the CLOUD Act and speak to more incremental processes of normative change that entrench the vision of a security partnership in data governance. There seems to be underlying consensus based on close interaction, even the formation of a “community, where everybody knows each other” (Tech company employee A, personal communication, 2019). Critical voices have problematized that the proposals are likely to shift due process functions from judicial authorities to companies (NGO policy officer, 2018, personal interview). While Microsoft failed to change law enforcement practices, it was able to significantly reduce legal uncertainty and successfully established itself as both a responsible company engaged to protect consumers from harm (Smith 2018a) and a “critical check to ensure that governments’ use of their investigative powers strictly adhere to the rule of law” (Smith 2018b, 2). This establishes Microsoft as a serious challenger of (illegitimate) public jurisdictional claims.

In conclusion, while the conflict became prominent internationally due to the underlying conception of data governance as relevant to sovereignty and privacy, data were increasingly referred to as a tool in the fight against (trans)national crime in the aftermath of the court case. This required cooperation rather than the protection of sovereign interest. Thus, while the initial challenge drew on principles articulated in the local liberal vision of data governance, the goals of legal certainty, globalist solutions, and security converged to promote a vision of security partnership. This is likely to support the expansion rather than limitation of data sharing in the long run.

Right to Be Forgotten

The third case relates to the “right to be forgotten” or “right to erasure” (Regulation (EU) 2016/679 (GDPR), Art 17), which has been contested in both content and scope. The jurisdictional conflict emerged at the intersection of public/private and local/global jurisdictional claims of control over data. The right to be forgotten first became a topic of debate in 2009 when Spanish citizen Mario Costeja Gonzáles filed a complaint with the Agencia Española de Protección de Datos (AEPD) after unsuccessfully trying to get information on home-foreclosure notices removed from the internet. The Spanish data protection authority (DPA) argued that data subjects have the right to request the delisting of such information from search engines results, as this would dramatically decrease the likelihood of accidental access. The search engine Google challenged this decision, and the case was brought before the CJEU. The Court found in favor of the AEDP’s request under the condition that the data are “inadequate, irrelevant or no longer relevant, excessive in relation to the purposes of the processing” (CJEU 2014, 19). The global relevance of the case manifested through clashing jurisdictional claims regarding the scope of its application by Google and the French Commission nationale de l’informatique et des libertés (CNIL). The French DPA took issue with Google’s interpretation that requests should only be removed from European Google domains, such as google.fr or google.co.uk and requested their global removal (2015). The case again was referred to the CJEU on 25 July 2017 and a judgment in favor of Google was issued in September 2019. The judgment, however, is open to the possibility of diverging national regulation.

Making the Object of Governance

For Google, there are significant incentives not to restrict search results and avoid the responsibility of adjudicating
on a significant number of requests.\footnote{Google currently delists 52.3 percent of URLs based on over 1,000,000 removal requests (Google 2021).} However, Google’s strategy in the first CJEU case was mainly based on the assumption that the Court could not claim jurisdiction, as the data processing was conducted by Google Inc., based in the United States rather than Google Spain. Rather than formulating a competing jurisdictional claim in reference to a governable object, community, or normative justification, Google thereby simply denied the legitimacy and effectiveness of the EU’s jurisdiction based on its compliance with US law (Google Spain and Google, Inc. 2012, paras. 2–4). The Court did not recognize this line of reasoning. In its judgment, the CJEU strongly focused on the implications of data protection and privacy for the individual arguing that such rights “override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject’s name” (CJEU 2014, 17).

This is in line with an increasing conceptualization of data as an individual rights concern in the EU, as pointed out by EU Justice Commissioner Reicherts arguing that “handling citizens’ personal data brings huge economic benefits to them [companies]. It also brings responsibility” (2014). In the aftermath of the case, Google actively tried to shape the discourse drawing on its economic resources and the capacity for swift action. The company quickly complied with the ruling and delisted the search results domestically. It installed an advisory council to develop removal guidelines, which established its identity as a responsible and impartial actor. The company’s lobby spending increased by 240 percent between 2014 and 2017 with reports declaring 200 meetings with high level EU officials since 2014 (Kergueno 2017).

Neither the 2014 judgment nor the GDPR specified the geographical scope of delisting or removal under the right to be forgotten. Nonetheless, the CNIL made a jurisdictional claim based on EU data protection law. It requested the global removal of links arguing that the delisting must be effective without restriction for all processing, even if it conflicts with foreign rights (CNIL 2016 (translation)). This entrenched a local liberal vision of data governance in reference to a community of EU citizens.

In summary, in the initial phase of jurisdictional conflict, Google failed to make a substantive justification of its jurisdictional claim based on its perceived formal legal status outside the CJEU’s jurisdiction. This failed to be recognized by a court that emphasized the rights-based character of data. The CNIL strongly tied this rights-based conceptualization of data to the local reference community to enforce a local law globally to protect domestic rights.

**Responses and Justifications**

In response to the CNIL’s jurisdictional claim, Google agreed to delisting search results if the IP address indicates the user location in the EU. However, the company appealed the fine of €100,000 imposed by the CNIL in 2015 and refused to delist globally, which the French High Court referred to the CJEU in 2017. Compared to the first court case, Google significantly changed its strategy to increase its reliance on normative arguments and closer interaction with different local stakeholders (Tech company employee, 2019, personal interview). Google began to strongly emphasize the fundamental right status of freedom of speech, pointing to the potential rise of censorship and threats to free access to data. Chief Legal Officer Walker argued that the proceedings “represent a serious assault on the public’s right to access lawful information” (Walker 2017). The company was successful in countering the public approach insofar as not only a broad coalition of businesses, such as Microsoft, but also NGOs have supported the approach. For instance, an amicus brief criticized that “by consistently framing freedoms and rights negatively affected by the right of delisting as ‘interests’ […] the balancing conducted by the Court of Justice would be tilted towards the right to data protection from the very beginning” (RCFP and Others 2017, 13). Google successfully created a conceptualization of data that was similarly rights-based, but emphasized the collective nature of data as a common resource. This established a vision of global protection and public access to information rather than the right to privacy as the dominant interpretation.

**Outcome**

The right to be forgotten has been strengthened with the EU’s GDPR, which to some extent constitutes a loss for Google. In its recent judgment, however, the Court generally followed the opinion that EU law does not currently cover a global enforcement of the right to be forgotten (CJEU 2019, paras. 61–7). While this seems to endorse the global protection vision voiced by Google, the judgment emphasized that specific communities or states may implement legislation to demand global delisting in the future. The CJEU thereby provided a legitimation to strengthen privacy or freedom of access rights depending on the specific balancing acts performed by legislators or DPAs. Therefore, this has strengthened a vision of data governance as the sovereign right of communities rather than its global character.

In conclusion, the judgment has reinforced the idea that rather than perceived as fragmentation, the normative differences between communities should be embraced. While the court case indicates a win for Google’s representation as a responsible actor, it might challenge transnational company practices in favor of a division of rules in the long term.

**Discussion**

This paper has presented three illustrative cases of conflict in the field of transnational data governance. I have argued that in addition to the well-explored institutional and power dimensions of these conflicts, their character as conflicts over meaning is undertheorized. These divisions persist across issue areas and over time and therefore offer insights into the longer-term trajectory of data governance. While actors are united by the tacit understanding that foundational societal problems are at stake, the analysis has specified four fundamentally distinct conceptualizations of the object, reference community, and broader societal goals of data governance as depicted in table 1 earlier. Table 2 demonstrates that the dividing lines mainly run between the local liberal and the security partnership vision of data governance. This has strong similarities to the privacy versus security divide that is alluded to in the literature but is more complex. Jurisdictional claims were only successfully articulated when actors combined the more substantive justifications based on privacy or security with the more procedural justifications of sovereignty or globalism, respectively. Justifications based on the vision of a digital economy seemed to have provided added support for the vision of a security partnership, as proponents of both visions tend to favor looser rules at the global level. In all
exemplary cases, actors referred to this vision, indicating its significance. While many actors articulated justifications in line with the vision of global protection, these were rarely decisive for the outcome of the conflict.

The overview over the cases also highlights that the outcome of the conflict not only depends on the invoked governance visions but also indicates several relevant factors, including the institutional context (Fahey and Terpan 2021). Nonetheless, the extent to which agreements represents a compromise between competing visions, for example through the inclusion of additional oversight or review mechanisms, seems to influence the stability of the agreement. Through increased transparency requirements and references to the rights-based conceptualization of data, bulk surveillance practices strongly based on the conceptualization of data as a tool have expanded, as highlighted by the PNR case (Bellanova and De Goede 2020). This also illustrates how legal measures not only constrain but also specifically enable data use practices (Cohen 2019).

The cases also indicate that agreements tilting heavily toward one vision are vulnerable to disruption by actors that draw on principles consistent with an alternative conceptualization of data. Jurisdictional overlap seems to have an empowering effect on non-state actors and actors with (formally) more marginal positions. High-stakes agreements were disrupted successfully due to individuals, such as Schrems in the first example, or companies, such as Microsoft in the third example. In contrast to the suggestion by Faude and Große-Kreul (2020), who find overlap to empower marginalized actors in their own organization, this effect is particularly relevant vis-à-vis actors in other jurisdictions. As demonstrated in the Safe Harbor case, non-state actors were able to disrupt transatlantic data sharing practices more significantly than domestic activities, as the largely unobstructed intelligence activities by EU member states show (Farrell and Newman 2019).

These challengers frequently draw on the local liberal vision of data governance. Thereby, they often antagonize particularly private companies from the United States. In interviews, private company representatives describe “discrimination” (Tech company employee, 2019, personal interview) and “harmful protectionism” (Private sector representative, 2019, personal interview) against US-based companies. In the public sector, the predominantly domestic or local character of governance bodies, such as data protection authorities, and laws, such as the 1995 Data Protection Directive, has left an ideational legacy whereby public authorities tend to reproduce their specific local focus globally, even in disregard of competing local norms or alternative conceptualizations of data. While it empowers individual rights, this approach collides with field-inherent restrictions to sovereignty based on the transnational nature of data transfers. It tends to produce unstable agreements and exacerbate conflicts (see critically Kuner 2015), as demonstrated in the right to be forgotten case. The case also demonstrates that even rights-based conceptualizations of data are not necessarily compatible if there is disagreement concerning the hierarchization of fundamental rights, such as privacy and freedom of speech, the locus of governance, or the public or private character of governance.

Throughout the cases, private companies acted as both challengers and stabilizers of the status quo. While in the first two cases, private companies were less visibly engaged in meaning making processes, the right to be forgotten case and the Microsoft case showed how corporate advocacy relied on a combination of material resources and active participation in object construction processes. Big tech companies attempted to create narratives about their legitimate behavior and even explicitly called for regulation. At the same time, they criticized competitors’ exploitative data practices (Hern 2019) and increased their lobbying activities (Kergueno 2017). By challenging jurisdictional claims from public authorities and actively shaping the rules, they seem to some extent displayed characteristics of what Eichensehr has termed “Digital Switzerlands” (2019), in the sense that they attempted to shape governance and scrutinize the exercise of public power. In the examples earlier, companies were more successful in jurisdictional conflicts when they actively attempted to make claims that established their responsibility to shape policy making and protect individual rights. They were less successful when attempting to avoid responsibility, as Facebook in the first example. Nonetheless, while companies seem to embrace the concept of responsibility, they have so far been more hesitant to embrace accountability for their actions, which makes a characterization as Digital Switzerland seem premature.

Conclusion

The aim of this article was to understand the prevalence of disruptive conflicts in transatlantic data governance. Drawing on a sociological approach, I have argued that these conflicts are indicative of and amplified by deep normative divisions: While united by a common perception that data governance is important, actors co-create distinct conceptualizations of data that are embedded in different value and justificatory systems. Building on this assumption, I have identified four justificatory bases co-created through jurisdictional claims. While proponents of social interaction driven by the belief in security or economic progress tend to promote loose governance structures at the global level, those focusing on data as an individual rights concern demand increasing legislative control on the domestic or community level. In contrast, proponents of a vision of global coherence and cooperation propose medium interoperable or global protection measures.

The theorization of these different conceptualizations of data governance is tentative and requires additional empirical research. How do, for example, conceptualizations in China or India differ from those presented in this paper?
How do claims of control play out in alternative policy areas, such as health? In the current COVID-19 crisis, the importance of conceptualizing governable objects to realize governance goals for specific communities is particularly evident. Whether data are conceptualized as a neutral tool in the fight against an existential threat or as an important part of human dignity impacts assessment of proportionality and necessity in the pandemic’s data governance practices. But what can data actually achieve in terms of solving problems or addressing security threats? While there is no shared understanding of the societal problems that are to be addressed by engaging in data governance, even challenging actors, such as the EP or Microsoft, rarely question the idea that data can provide an answer to these problems. Due to this faith into “dataism” (van Dijck 2014) or “solutionism” (Nachtwey and Seidt 2020), actors are frequently complicit in the creation or institutionalization of structures and policies that undermine their wider normative agenda, which amplifies conflicting developments.

This makes the conceptual contribution of the paper so important, focusing on the multidimensional quality of jurisdictional claims as institutional, power-driven, legal, and normative claims. Who are the winners and losers from specific conceptualizations of data? The paper’s focus on jurisdictional claims naturally limits the analysis to the carefully curated representations of the involved actors. While the inclusion of diverse data sources, including interviews and leaked documents, addresses some of these limitations, other aspects, such as the overt exercise of power or control through data infrastructures (Bellanova and de Goede 2020), need further research. While de Goede has explored the role of banks and airlines as “reluctant security actors” (Farrell and Newman 2019), need further research. While de Goede has explored the role of banks and airlines as “reluctant security actors” (Farrell and Newman 2019), empirical cases also demonstrate the importance of further conceptualizing private agency and perceptions of private responsibility in public data management processes.

In addition, the paper’s scope is limited to a community of experts. Further research drawing on newspaper articles and opinion polls could incorporate the visions of a broader public, pointing to potential differences and the salience dynamics of those visions. This is relevant, because jurisdic- tional overlap may obfuscate the decision-making processes between conflicting norms for affected stakeholders (Johns and Compton 2019, 16). The emerging literature that considers not only the foundational societal consequences of contemporary data use (Zuboff 2018) but also the underlying legal (Mitsilegas 2014; Cohen 2019) and power structures (Farrell and Newman 2019), and data-based value judgments (Aradau 2020) is therefore just a first step toward a more comprehensive analysis of competing normative goals in transnational data governance.

Where does this leave us in terms of the future development of transnational data governance? Jurisdictional conflicts are unlikely to disappear when regulatory measures, such as the GDPR, strengthen the extraterritorial reach of governance provisions. As the geopolitical relevance of data and internet governance increases, the stakes seem to be higher than ever. While jurisdictional conflicts have a productive dimension, they require substantial improvements in terms of access. As the success of Schrems demonstrates, the EU legal order gives significant access opportunities to resourceful individuals but large parts of the conflicts analyzed play out behind closed doors. Kosta (2020) also raises the limits of human agency when faced with machine-based data processing and the targeting of groups rather than individuals. Better data governance requires a broader debate on the construction of data analysis as an opaque and highly complex practice that is moved out of public debate.

**Supplementary Information**

Supplementary information is available at the *International Studies Quarterly* data archive.

**References**

ABHITT, ANDREW. 1986. “Jurisdictional Conflicts: A New Approach to the Development of the Legal Professions.” *American Bar Foundation Research Journal* 11 (2): 187–224.

———. 1988. *The System of Professions: An Essay on the Division of Expert Labor*. Chicago: The University of Chicago Press.

———. 2005. “Linked Ecologies: States and Universities as Environments for Professions.” *Sociological Theory* 23 (3): 245–74.

ALLAN, BENTLEY B. 2017. “Producing the Climate: States, Scientists, and the Constitution of Global Governance Objects.” *International Organization* 71 (1): 131–62.

AMOORE, LOUISE. 2020. *Cloud Ethics*. Durham: Duke University Press.

AMOORE, LOUISE, AND RITA RALEY. 2017. “Securing with Algorithms: Knowledge, Decision, Sovereignty.” *Security Dialogue* 48 (1): 3–19.

ARADAU, CLAUDIA. 2020. “Experimentality, Surplus Data and the Politics of Debilitation in Borderzones.” *Geopolitics*, December, 1–21.

BAZACQ, THERER. 2007. “The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies.” *JCMS: Journal of Common Market Studies* 46 (1): 75–100.

BELLANOVA, ROCCO, AND MARIEKE DE GOEDE. 2020. “The Algorithmic Regulation of Security: An Institutional Perspective.” *Regulation & Governance*. https://doi.org/10.1111/rego.12358.

BENNETT, COLIN JOHN, AND CHARLES D. RAAB. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge: MIT Press.

BIGNAMI, FRANCESCA, AND GIORGIO RESTA. 2015. “Transatlantic Privacy Regulation: Conflict and Cooperation.” *Law & Contemporary Problems* 78 (4): 231–66.

BOETTCHER, MIRANDA. 2020. “Cracking the Code: How Discursive Structures Shape Climate Engineering Research Governance.” *Environmental Politics* 29 (3): 890–916.

BOEDRINSKI, LUC, AND LAURENT THÉVENOT. 2006. *On Justification: Economies of Worth*. Translated by C. Porter. Princeton Studies in Cultural Sociology. Princeton: Princeton University Press.

BRADFORD, ANN. 2020. *The Brussels Effect: How the European Union Rules the World*. USA: Oxford University Press.

BUXBAUM, HANNAH L. 2009. “Territory, Territoriality, and the Resolution of Debilitation in Borderzones.” *Security Dialogue* 40 (1): 63–75.

BUZAN, BARRY, OLE WAER, AND JAAP DE WILDE. 1998. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers.

CJEU. 2014. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Court of Justice: General Court. 2015. Schrems v Data Protection Commissioner. Court of Justice: General Court.

———. 2019. *Google LLC, successor in law to Google Inc., v Commission nationale de l’informatique et des libertés (CNIL)*. Court of Justice: General Court.

———. 2020. *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems*. Court of Justice: General Court.

CNIL. 2015. “CNIL Orders Google to Apply Delisting on All Domain Names of the Search Engine.” December 6, 2015. https://www.cnil.fr/fr/node/15790.

———. 2016. “Délibération N°2016-054 Du 10 Mars 2016.” https://www.cedelfrance.gouv.fr/affichCnil.do?id=CNILTEXT000032291946.

COE. 2018. “Octopus Conference 2018: Key Messages.” Strasbourg. http://rm.coe.int/3021-90-octo18-keymessages/16808e67b.

COHEN, JULIE E. 2019. *Between Truth and Power: The Legal Constructions of International Capitalism*. USA: Oxford University Press.

DASKAL, JENNIFER. 2018. “Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0.” *Stanford Law Review* 71: 9–16.

DAVIS, SARA E. AND CLARE WENHAM. 2020. “Why the COVID-19 Response Needs International Relations.” *International Affairs* 96 (5): 1227–51.
FAHEY, E. LAINÉ, AND FABIEN TERPAN. 2021. “Torn Between Institutionalisation and Europeanisation.”

EUROPOL. 2019. “SIRIUS EU Digital Evidence Situation Report 2019.”

———. 2018b. “Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters.” COM(2018) 225 final.

ECIPE. 2015. “The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce. A Trade Impact Assessment of the General Data Protection Regulation (GDPR) by the European Centre for International Political Economy (ECIPE) for the U.S. Chamber of Commerce.”

https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_Lr.pdf.

EFAT, A. SIF, AND ABRAM L. NEWMAN. 2016. “Deciding to Defer: The Importance of Fairness in Resolving Transnational Jurisdictional Conflicts.” International Organization 70 (2): 409–41.

EICHIENSER, KRISTEN. 2019. “Digital Switzerland.” University of Pennsylvania Law Review 167: 665–792.

EP. 2014. “Resolution on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens’ Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs (2013/2188(INI)).” P7_TA(2014)0230. Strasbourg.

EUROPOL. 2019. “SIRIUS EU Digital Evidence Situation Report 2019.” The Hague. https://www.europol.europa.eu/sites/default/files/documents/sirius_eu digital_evidence_report.pdf.

FAHEY, ELAINE, AND FAREH TERRAN. 2021. “Torn Between Institutionalisation and Judicialisation: The Demise of the EU-US Privacy Shield.” Indiana Journal of Global Legal Studies 28 (2): 205–44.

FAKII, HENRY, AND ABRAM L. NEWMAN. 2019. “Of Privacy and Power: The Transatlantic Struggle over Freedom and Security.” Princeton: Princeton University Press.

FARRELL, HENRY, AND ABRAM L. NEWMAN. 2019. “The MNC-Coalition Paradox: Issue Salience, Foreign Firms and the General Data Protection Regulation.” International Political Sociology 15 (3): 296–314.

FARRELL, HENRY, AND ABRAM L. NEWMAN. 2017. “Algorithmic State Surveillance: Challenging the Notion of Agency in Human Rights.” Regulation & Governance. https://doi.org/10.1111/rego.12531.

KENNER, CHRISTOPHER. 2015. “Extra-territoriality and Regulation of International Data Transfers in EU Data Protection Law.” International Data Privacy Law 5 (4): 235–45.

LEIPOLD, SINA, PETER H. FEINTZ, GEORG WINKEL, AND REINER KELLER. 2019. “Discourse Analysis of Environmental Policy Revisited: Traditions, Trends, Perspectives.” Journal of Environmental Policy & Planning 21 (5): 445–63.

MCCOURT, DAVID M. 2016. “Practice Theory and Relationalism as the New Constructivism.” International Studies Quarterly 60 (3): 475–85.

MITSELAGAS, VASSILIS. 2014. “Transatlantic Counterterrorism Cooperation and European Values: The Elusive Quest for Coherence.” In A Transatlantic Community of Law: Legal Perspectives on the Relationship between the EU and US Legal Orders, edited by Elaine Fahey and Deirdre Curtin, 289–315. Cambridge: Cambridge University Press.

MOODY, GLEN. 2016. “In ‘an Unusual Move,’ US Government Asks to Join Key EU Facebook Privacy Case.” Ars Technica, June 13, 2016. https://arstechnica.com/tech-policy/2016/06/ eu-facebook-schrems-case-us-government-amicus-curiae/.

NATIONAL INSTITUTE OF LEARNING DISABILITIES. 2016. “Practice Theory and Relationalism as the New Constructivism.” International Studies Quarterly 60 (3): 475–85.

OKIEN, ROBERT. 2014. “Regulatory Governance: Rules, Advances in Sociology. London; New York: Routledge; Taylor and Francis Group.

KERGUNO, RAFAEL. 2017. “The Uber-Lobbyists: How Silicon Valley Is Changing Brussels Lobbying.” Transparency International EU. May 4, 2017. https://transparency.eu/uber-lobbyists.

KJER, POUL F., AND ANSTEY VETTERLEIN. 2018. “Regulatory Governance: Rules, Resistance and Responsibility.” Contemporary Politics 24 (5): 497–506.

KNORE-CITINA, KARIEN. 1999. Epistemic Cultures: How the Sciences Make Knowledge. [1. publ.]. Cambridge: Harvard University Press.

KONTA, ELENI. 2020. “[Algorithmic State Surveillance: Challenging the Notion of Agency in Human Rights.” Regulation & Governance. https://doi.org/10.1111/rego.12531.

KONI, CHRISTOFER. 2015. “Extra-territoriality and Regulation of International Data Transfers in EU Data Protection Law.” International Data Privacy Law 5 (4): 235–45.

LEIPOLD, SINA, PETER H. FEINTZ, GEORG WINKEL, AND REINER KELLER. 2019. “Discurso Analysis of Environmental Policy Revisited: Traditions, Trends, Perspectives.” Journal of Environmental Policy & Planning 21 (5): 445–63.

MCCOURT, DAVID M. 2016. “Practice Theory and Relationalism as the New Constructivism.” International Studies Quarterly 60 (3): 475–85.

MITSELAGAS, VASSILIS. 2014. “Transatlantic Counterterrorism Cooperation and European Values: The Elusive Quest for Coherence.” In A Transatlantic Community of Law: Legal Perspectives on the Relationship between the EU and US Legal Orders, edited by Elaine Fahey and Deirdre Curtin, 289–315. Cambridge: Cambridge University Press.

MOODY, GLEN. 2016. “In ‘an Unusual Move,’ US Government Asks to Join Key EU Facebook Privacy Case.” Ars Technica, June 13, 2016. https://arstechnica.com/tech-policy/2016/06/ eu-facebook-schrems-case-us-government-amicus-curiae/.

NATIONAL INSTITUTE OF LEARNING DISABILITIES. 2016. “Practice Theory and Relationalism as the New Constructivism.” International Studies Quarterly 60 (3): 475–85.

OKIEN, ROBERT. 2014. “Regulatory Governance: Rules, Advances in Sociology. London; New York: Routledge; Taylor and Francis Group.

RUBBER, PEDRO. 2015. “Statement from U.S. Secretary of Commerce Penny Pritzker on European Court of Justice Safe Harbor Framework Decision.” Department of Commerce. October 6, 2015. https://wwwocommunications.gsa.gov/safeguard-executive-summary-2015-10.

PITZKER, PENNY. 2015. “Statement from U.S. Secretary of Commerce Penny Pritzker on European Court of Justice Safe Harbor Framework Decision.” Department of Commerce. October 6, 2015. https://www.commerce.gov/news/press-releases/2015/10/ statement-us-secretary-commerce-penny-pritzker-european-court.

RABB, CHARLES, AND IAN SZEKELY. 2017. “Data Protection Authorities and International Data Privacy Protection.” Computer Law & Security Review 33 (4): 421–33.

RGFP AND OTHERS. 2017. “Statement in CJEU Case C-507/17.” Accessed September 6, 2021. https://www.rgfd.org/wp-content/uploads/imports/2017-11-29-Statement-CJEU-in-Googles-CNIL-RGFPetal-ansfiled.pdf.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Personal Data with Respect to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC. 2016.

REICHERTS, MARTINE. 2014. “The Right to Be Forgotten and the EU Data Protection Reform.” Lyon: IFLA World Library and Information Congress. http://europa.eu/rapid/press-release_SPEECH-14-568_en.htm.

REIDENBERG, JOEL R. 2000. “Resolving Conflicting International Data Privacy Regimes of Algorithmic Regulation.” Indiana Law Review 33 (4): 1315–97.

RUFFET, ELYNN, ENNIS ISIN, AND DEIDER BREG. 2017. “Data Politics.” Big Data & Society 4 (2): 2053951717717749.

RUGENGER, CEDRIC. 2015. “Symposium Issue on Extraterritoriality and EU Data Protection.” International Data Privacy Law 5 (4): 221–5.

SCHREMS, MAXIMILIAN. 2015. “To the Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois, Ireland. Complaint Against Facebook Ireland Ltd –23 ‘PRISM.’” June 25, 2013. http://www.europewww.facebook.com/prism/facebook.pdf.

SCHÜMANN, WOLF J., AND MAX-OTTO BAUMANN, eds. 2017. Privacy, Data Protection and Cybersecurity in Europe. Cham: Springer.

SENDING, OLE JACOB. 2015. The Politics of Expertise: Competing for Authority in Global Governance. Ann Arbor: University of Michigan Press.
Smith, Brad. 2018a. “The CLOUD Act Is an Important Step Forward, But Now More Steps Need to Follow.” Microsoft on the Issues (blog). April 3, 2018. https://blogs.microsoft.com/on-the-issues/2018/04/03/the-cloud-act-is-an-important-step-forward-but-now-more-steps-need-to-follow/.

———. 2018b. “A Call for Principle-Based International Agreements to Govern Law Enforcement Access to Data.” Microsoft on the Issues (blog). September 11, 2018. https://blogs.microsoft.com/on-the-issues/2018/09/11/a-call-for-principle-based-international-agreements-to-govern-law-enforcement-access-to-data/.

Stroup, Sarah S, and Wendy H Wong. 2017. The Authority Trap: Strategic Choices of International NGOs. Ithaca: Cornell University Press.

Supreme Court of the US. 2018. “Oral Hearing in the Supreme Court of the United States United States, Petitioner, v. Microsoft Corporation, Respondent.” No 17-2. Washington, D.C.

Ulbricht, Lena. 2018. “When Big Data Meet Securitization. Algorithmic Regulation with Passenger Name Records.” European Journal for Security Research 3 (2): 139–61.

UNCTAD. 2020. “Data Protection and Privacy Legislation Worldwide.” https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

US. 2017. “In the Matter of United States v. Microsoft Corp.: Petition for a Writ of Certiorari.” No 17-2. Supreme Court of the US.

van Dijk, José. 2014. “Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology.” Surveillance & Society 12 (2): 197–208.

van Puyldee, Damien, Stephen Coulthart, and M. S. Shahriar Hossain. 2017. “Beyond the Buzzword: Big Data and National Security Decision-Making.” International Affairs 93 (6): 1397–416.

Walker, Kent. 2017. “Defending Access to Lawful Information at Europe’s Highest Court.” November 15, 2017. https://www.blog.google/around-the-globe/google-europe/defending-access-lawful-information-europes-highest-court/.

Yeung, Karen. 2018. “Algorithmic Regulation: A Critical Interrogation.” Regulation & Governance 12 (4): 505–23.

Zuboff, Shoshana. 2018. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. London: Profile Books.