2024

Extraterritoriality

Francesca Bignami

Giorgio Resta

EXTRATERRITORIALITY

Francesca Bignami & Giorgio Resta

Oxford Handbook on Digital Constitutionalism (Giovanni De Gregorio, Oreste Pollicino & Peggy Valcke eds., forthcoming)

ABSTRACT

This chapter argues that the competing American ballot-box and European fundamental rights paradigms of regulatory law have marked the specific domain of digital regulation. These regulatory paradigms and their associated state interests are projected extraterritorially through the market power of Silicon Valley, on the one hand, and the privacy rights of European Union (EU) regulators, on the other hand. This chapter also analyzes recent developments in the EU, where there is now a state effort to make digital markets and, relatedly, an emerging preference for some data localization to promote both fundamental rights *and* economic and security interests. In China, we observe the emergence of a layered form of digital regulation: at the deepest level is state control of digital infrastructure, industry actors, and civil society users; layered on top is an attempt to improve the position of consumers through both digital platform regulation and competition law applied to the largest oligopolies. As a result, the earlier Chinese strategy of data localization is now complemented by a bureaucratically controlled form of extraterritorial engagement.

I. INTRODUCTION

How the law says that markets should be regulated differs dramatically across the globe. In the American ballot-box paradigm of public law, government adherence to procedural norms of free and fair elections, separation of powers, accountability to the elected branches, and public participation in administrative policymaking is the key to the right and good regulation of markets. Constitutional law has relatively little to say about the operation of markets and civil society, thought to be intrinsically liberty-affirming. By contrast, in the European paradigm of public law, fundamental rights of all stripes are crucial—legislators and regulators, as a matter of law, are required to abide by negative rights such the right to trade, positive rights, such as the right to health care, and everything in between, such as affirmative action in the name of equal treatment. If anything, these two paradigms have been especially pronounced in government regulation of the internet. They have also been especially apparent to outside observers because of the clashes that have been generated in transatlantic relations between the ballot-box and fundamental rights models. The borderless world of the internet has time and time again brought the two paradigms of regulatory law face to face and the result has been a string of temporary accommodations that have been prone to unraveling and renegotiation.

Whether the projection of these approaches to digital governance beyond core fact patterns of territoriality is indeed extraterritorial is a matter of debate. “Extraterritoriality” has negative connotations that imply the illegitimate assertion of the state’s authority to prescribe, adjudicate, and enforce.[1] Yet the field of conflicts of law has always operated with a variety of approaches to the question of when a jurisdiction may rightfully assert authority over, and apply its law to, transactions and events that span more than one country. In the criminal domain,

passive personality jurisdiction allows for prosecutors and courts to assert their law and jurisdiction regardless of where the crime occurred if the purpose is to exact retribution for harms done to their citizens.[2] In the law of torts, it is generally the law of the place of the accident that applies, while the court with jurisdiction is that of the defendant tortfeasor. With respect to immovable property, the jurisdiction with control over disputes is generally the place where the property is located. The list could go on and on, with multiple permutations of choice of law and the jurisdiction of courts. And, of course, the list would look different depending on which nation's conflicts of law doctrine was being surveyed. The basic point is that even in the physical world, events that implicate multiple countries—think for example antitrust—give rise to a variety of rules on which law and which forum govern those events.

When we turn to the virtual world, the difficulty of locating the geographic center of human interactions is multiplied exponentially because of how the physical backbone of the internet operates and because of the ease and speed with which data moves across the network. By design, when a single communication moves through the network, it is split into multiple packets and routed through multiple servers that may very well be located in multiple jurisdictions. It does so in milliseconds and indeed, in the future, perhaps at the speed of light. The location of storage and processing of the enormous quantities of data generated in even the simplest of transactions is determined more by the business reasons of the particular corporate actor than by virtue of proximity to the users of their services.

In light of the difficulties inherent in the concept of extraterritoriality, this chapter takes a pragmatic approach and focuses on the application of the law – or the potential effects of that law – beyond the most local, and territorially rooted, of fact patterns. That core case of squarely territorial application of law is a digital communication between two actors who are located in the same jurisdiction and a digital communication that is routed between servers in that territory and that is stored in that same territory. Any other type of communication, where one of the individuals is located abroad, one of the servers through which the communication is routed is located abroad, or one of the servers on which the communication is stored and processed is located abroad, is a communication to which the application of the jurisdiction's law, court proceedings, and enforcement powers is potentially extraterritorial.

As was indicated above, there are multiple reasons and opportunities, many of which are entirely legitimate from the traditional perspective of conflicts of law, for countries to project their distinct regulatory paradigms to digital communications with a foreign component. In this chapter, we isolate the critical features of the distinct paradigms. We then turn to how they have been projected abroad in the course of regulating the digital world. We also consider how traditional areas of law, such as the enforcement of criminal law, which are not specifically targeted at digital governance, have acquired an extraterritorial dimension by virtue of the transformations wrought by the internet.

The discussion below intersects with the larger project of this book. We consider many of digital constitutionalism's developments in the state, societal, and global domains. Perhaps driven by the Chapter's topic, our account of digital governance begins from the state (which in the case of the EU operates at the regional level). The normative template developed at the state level for political organization, markets, and civil society actors is then projected abroad or used as a shield against foreign actors. By no means are such norms developed in isolation from the rest of the world, but at least with respect to the three jurisdictions that we cover (the US, the EU,

and, briefly, China), they are still strong enough to require adherence, internally, to their distinct legal approaches and to promote them externally in their dealings with foreign actors.

This Chapter proceeds as follows. Following the introduction, Section Two focuses on the United States. Section Three covers the European Union. We would be remiss if we failed to consider the emerging digital superpower, China. Therefore, Section Four briefly traces the regulatory model emerging in China, followed by concluding thoughts on the three jurisdictions.

II. UNITED STATES

In the United States, regulating market actors, including the companies that are central to today's digital space, has traditionally followed what, in a previous work, one of us has called a "ballot-box democracy" paradigm of public law.[3] In the American ballot-box paradigm, the law is focused on promoting democratic proceduralism in the political branches, the bureaucracy, and the courts. Markets and civil society are mostly left alone, on the theory that they are intrinsically liberty-affirming.

In the digital space, the ballot-box paradigm has been particularly evident, and it has been entrenched through the twin dynamic of privacy rights (or the lack thereof) and free speech rights. At the constitutional level, privacy is only protected against state actors and even in the public domain, the Supreme Court has been quite stingy with respect to *data* privacy.[4] In the legislative domain, an omnibus privacy law applicable to the public sector, i.e. the Privacy Act of 1974, was passed early on.[5] But in the private sector, the United States has never adopted a comprehensive approach to data privacy regulation, preferring sector-specific laws that have been incapable of responding to broader developments in the tech industry.[6] Combined with the political economy of American consumerism, this lax approach to marketplace privacy gave rise to the e-commerce boom of the 1990s and 2000s.[7] Behind the American consumer is easy consumer lending and behind easy consumer lending are the credit reporting services of the mammoth corporations Equifax, Experian, and Transunion. Their unfettered access to, and exchange of, the personal information collected by all types of businesses, originally for purposes of extending consumer credit, was later engineered into the digital practices of American internet firms. Data brokers and digital advertising exchanges are vital to bringing down costs for the physical goods and digital services provided over the internet. E-commerce's hallmark of free content and expanded consumer choice are difficult to imagine without the continuous and pervasive monetization of personal data that has been made possible by the absence marketplace privacy rights and regulation.

By contrast with the right to privacy, the right to free speech has been very prominent in the operation of civil society and the marketplace. To begin with the constitutional right, the Supreme Court has placed the First Amendment's right to speech at the top of the hierarchy of constitutional rights because, like the right to vote and the right of peaceful assembly, it is vital to democratic deliberation and "those political processes which can ordinarily be expected to bring about repeal of undesirable legislation."[8] Speech is also thought to be a particularly important right because of the metaphor of the marketplace of ideas, originally espoused by Justice Oliver Wendell Holmes: "the best test of truth is the power of the thought to get itself accepted in the competition of the market."[9] Although speech, like other constitutional rights, only applies to state action, the Court early on took a quite flexible approach to finding state action in the famous libel case of *New York Times Co. v Sullivan*,[10] and as a result, the so-called "public figure" doctrine operates as a shield in many common law (private) defamation actions.[11]

At the legislative level, Section 230 of the Communications Decency Act of 1996 operates as a "nearly impenetrable super-First Amendment for online companies."[12] The Act covers the issue of internet company liability for the speech of those that make use of their services, what today has evolved into social media platforms such as X and Facebook. One set of provisions criminalized indecent speech and materials sent over the internet. The other set is what is now codified in Title 47 Section 230 of the US Code and which gave immunity to platform companies for defamatory and other types of potentially illegal speech posted by their users, including if those platform companies engaged in content moderation (something which, if done by traditional media outlets, would render them liable for defamatory and other types of illegal speech). The provisions on indecency were promptly struck down by the Supreme Court as a violation of the First Amendment's guarantee of free speech.[13] In stark contrast with the indecency provisions, Section 230 soon was interpreted by the courts as an extraordinarily robust liability shield for platform companies. As Jeff Kosseff has persuasively argued, American internet companies would be much smaller and the digital economy would operate radically differently, without all of the third-party content that exists on the internet, in large part because of this federal law.[14] The social media boom, which really took off with the widespread adoption of portable smartphones around 2010, can be traced in large part to Section 230 and the prominence of speech rights in the American paradigm of ballot-box democracy.

How has this permissive regulatory approach to the digital world, with extensive protection for speech but not for other types of rights, been projected extraterritorially? The answer is to be found in the market dominance of American social media and e-commerce companies in combination with the borderless physical design of the network. Their business practices have shaped expectations of how the internet should operate and what is possible in the digital world: all personal data generated through digital communications can and should be monetized and all speech conveyed through digital platforms is worthy, at least as a first cut, of protection. In turn, these corporate practices and social expectations have spread extraterritoriality, well beyond US borders, to wherever the internet operates uncensored.

Ever since the EU passed the Data Protection Directive in 1996 and the E-Commerce Directive in 2000, there has been an effort to depart from this baseline and that effort has been ratcheted up with the General Data Protection Regulation (GDPR).[15] Just take two examples of European efforts to push back against the extraterritorial projection of the American regulatory paradigm—consent and the right to be forgotten. In the European regulatory paradigm of the fundamental right to privacy, the idea is that individuals should have to consent to the transfer of their data to data brokers and advertising exchanges and there is no end of doctrinal discussion as to whether consent is, or should be, "opt-in" or "opt-out." Yet no matter how valid one thinks control over one's personal data is as a policy matter, it is hard to deny that the consent pop-ups that routinely appear on websites today (linked to the website's privacy policy) are a source of irritation and are experienced as a barrier to getting to where the consumer wants to go. Most users perceive pop-ups as a set of boxes to click through and therefore, no matter how hard regulators try, they still do not operate as a genuine form of consent.

The same dynamic is apparent with the right to be forgotten. Privacy is generally conceptualized as one element of human dignity. Individuals have a right to stop others from talking about them and sharing facts about them even if those facts are true and even if, on a general level, it might be useful for the government or those with whom they have dealings to know those facts. This control over data is essential to the liberal notion of personhood and the

right for individuals to self-determine their own destinies. Obviously, individuals are members of society, and as such they have duties towards others including disclosing information about themselves that is important for society and the decisions that other individuals must make. What is relevant or irrelevant for others is one of the great challenges of liberal democratic theory. Today, however, in Europe and elsewhere, the fact of someone's sexual preference or the fact that someone was arrested but never charged or convicted of a crime are considered facts that should be irrelevant for others and therefore entirely for the individual to decide whether or not to reveal.

The vast possibilities of digital technology and the technical and regulatory design choices behind the rise of American internet companies have made it extraordinarily difficult to keep such information private. "Privacy is dead" is a common mantra of tech CEOs.[16] An early feature of the EU's countervailing regulatory approach was the right for individuals to require that information about their past that was no longer relevant for the present be anonymized or deleted.[17] It has since been reinforced in the GDPR's right to be forgotten. (Article 17). Under this provision of EU law, individuals have a right to request that search engines like Google and social media companies like Facebook erase or "take down" their personal data unless there are countervailing public interests or rights of freedom of expression. Today, after decades of case law and regulatory efforts, there are mechanisms in place in the big American internet companies that do business in Europe to remove personal information when so requested by the affected individual. However, just like the consent pop-ups and privacy policies that are ubiquitous on websites today, the removal of information can be a source of frustration for users of the internet. For instance, when Google complies with the European right to be forgotten and removes certain search results from its web browser, it also tells European users that there are additional results that they cannot see. The implication is that in the natural state of the digital world, as it exists in the American regulatory paradigm, there exists more information that is being withheld for mysterious and possibly illegitimate reasons from the eyes of the European public.

European regulatory requirements such as consent and the right to be forgotten come up against the regulatory and engineering baseline that is baked into the business practices of American internet industry and that has been projected extraterritorially by virtue of the open and interoperable architecture of the internet. They are often perceived, even to European citizens, as artificial constraints on a natural digital world—a world that, however, as should be clear from what has been written so far, has nothing natural to it but is an extraterritorial projection of the American regulatory paradigm. Constant, granular data about each and every digital citizen and available to all are not technological necessities, rather they reflect the way that the technology developed in Silicon Valley within a ballot-box democracy paradigm that paid a lot of attention to freedom of speech and little attention to other types of rights in the evolving technological space of the internet. It is certainly possible to imagine alternative forms of the commercial internet, in which the profits to be made are not derived from the ability to track consumers and monetize their data, but it will take a mammoth regulatory effort to transition to such an internet. It will require more than pop-up boxes, privacy policies, and take down notices floating above the deep-seated regulatory and technical design choices made in the early days of the (American) commercial internet.

The prominence of American internet companies has not only led to the projection abroad of the American regulatory model for the internet, it has also led to increased extraterritoriality of traditional areas of law. This has been particularly evident in criminal and national security law,

where the government has benefited from the centrality of American firms in the operation of the global internet to enforce American law in a variety of contexts where, pre-commercial internet, it would have been difficult or impossible to do so. There are a number of widely known transatlantic disputes that have resulted, two of which are discussed below.

In the domain of criminal law enforcement, the case of *United States v. Microsoft* and the subsequent CLOUD Act, illustrate how the global market power of companies like Microsoft can facilitate enforcement beyond purely local fact patterns. [18] In the Microsoft litigation, a federal prosecutor applied to a magistrate judge for a warrant under the Stored Communications Act (SCA) to compel Microsoft to produce emails relevant to a criminal investigation.[19] The emails were stored on a server not in the United States but in Ireland, but of course Microsoft controlled the data and could access it from its US headquarters. In the Court of Appeals, the government lost based on an interpretation of the relevant statutory provision, which the court found did not extend extraterritorially. By the time the case reached the Supreme Court, however, Congress had passed the CLOUD Act, which rendered the litigation moot, in favor of the government (which caused consternation in the European Parliament and among EU DPAs). The CLOUD Act makes it clear that the SCA warrant authority applies to all data stored by providers under US jurisdiction (which does not turn on place of establishment but on whether companies do business in the US), regardless of whether the servers are located in the US or abroad.[20] Under the long-standing definitions contained in the SCA, the types of services covered are "email providers, cellphone companies, social media platforms, and cloud storage services."[21] It goes without saying that the four largest internet companies outside of China, Google, Apple, Meta and Amazon, all provide services covered by the SCA and all are subject to US jurisdiction. Thus, by virtue of the global market power of its internet companies, the (extra)territorial reach of US criminal investigation and enforcement powers is vast.

The second example of extraterritorial reach comes from the enforcement of national security law. The Foreign Intelligence Surveillance Act (FISA) was enacted by Congress in 1978 to regulate government surveillance that is conducted inside the United States and that is targeted at "activities of foreign powers or their agents." FISA created a two-track scheme for foreign intelligence surveillance: one standard for US citizens and permanent resident aliens (collectively defined as "US persons" and protected by the Constitution's Fourth Amendment) and another, lower standard for non-resident aliens in the United States, such as those on tourist visas ("non-US persons" who were considered to have lesser Fourth Amendment rights). [22] With the revolution in digital technologies, as well as the changing national security environment, FISA has been amended repeatedly over the decades.[23] The most recent provisions are contained in the FISA Amendments Act of 2008.

The most salient FISA amendment for purposes of the extraterritoriality discussion is Section 702 (codified at 50 U.S.C. §1881a). [24] Section 702 applies to the collection of any type of digital communication, including real-time phone calls and emails, stored content such as emails and social media posts, and various types of metadata that identify such communications. It carves out a new category of persons for purposes of foreign intelligence surveillance: "persons reasonably believed to be non-US persons overseas." These are persons who, in contrast with non-US persons in the United States, have *no* Fourth Amendment rights. At the time of FISA's passage, in the pre-internet world, they would generally not have come within the technological capabilities of the government's surveillance operations on US territory. In the internet era, however, their bits are constantly and massively being routed through the US

communications network, to and from US electronic communications service providers, and they can and are the target of surveillance by the National Security Agency (NSA). Largely because those bits undoubtedly contain large quantities of US-person, as well as non-US person data, it was believed necessary to create a statutory authority with Fourth Amendment guarantees, i.e. Section 702. Section 702 is the legal basis for downstream collection (formerly called PRISM), the NSA program that collects content and metadata from a variety of internet companies. It is also the authority for upstream collection, the NSA program that intercepts personal data that transit through cables and switches coming into US territory, and that gathers both internet traffic and telephone calls, including the content of those communications.

Like the CLOUD Act, Section 702 has been the source of transatlantic conflict. In October 2015, in so-called Schrems I, the Court of Justice of the EU (CJEU) annulled the transatlantic agreement ("Safe Harbor") that had been used to provide the legal basis for commercial data transfers between the EU and the US as required under the EU Data Protection Directive (and discussed in the next section).[25] The reason was that the European Union had allowed an open-ended exception to Safe Harbor's data protection principles "to the extent necessary to meet national security, public interest, or law enforcement requirements"[26] without assessing the adequacy of the applicable legal framework.[27] The Court's decision was based in large part on the NSA's Section 702 programs that had been revealed by Edward Snowden in 2013. The successor agreement to Safe Harbor, Privacy Shield (2016), sought to address the Court's privacy concerns by detailing the legal limits on US surveillance powers and by creating an ombudsman, within the US State Department, with responsibility for the data subject access and redress guarantees of privacy law. Again, however, in the Schrems II judgment of July 2020, the CJEU annulled the US-EU agreement, again because it failed to guarantee privacy in the domain of national security surveillance, in particular in the NSA's Section 702 programs.[28] It remains to be seen whether the newly adopted EU-U.S. Data Privacy Framework (2023), which contains a far more independent form of redress as compared to the Privacy Shield ombudsman, will assuage European concerns.[29] For purposes of this chapter, the important thing to note is that, not unrelated to the intractability of the transatlantic dispute, Section 702 is the most extreme example of the extraterritorial projection of US power. It is surveillance of breathtaking scope that is designed to enforce a very common type of state law, national security, and that has been enabled by the physical design of the digital world and the market power of American multinationals in that world.

III. EUROPEAN UNION

In contrast with the United States, European democracies (which include the European Union), adhere to what one of us has called the fundamental rights paradigm of market regulation.[30] To be sure, democratic participation is also important in Europe. However, the legitimacy of government intervention in markets is tied more to adherence to fundamental rights directed at guaranteeing free and fair markets and civil society rather than respect for democratic proceduralism throughout the regulatory process. The fundamental rights paradigm is particularly evident at the judicial review phase. Laws, regulations, and other types of government action are tested for their respect for a variety of rights, including positive social rights, market freedoms, rights related to the environment, and rights connected to the digital sphere, including *both* the right to free expression and the right to personal data protection.

This European approach to market regulation has been in full display in the digital arena. What today falls under the umbrella of European "data law," a gamut of regulations dealing with

the collection and use of all sorts of data, has expanded outwards over the last two decades beginning from the essential core of personal data protection.[31] The original national laws of the 1970s and 1980s covered both government and market actors and were driven by an all-encompassing individual right to privacy. When the EU first took action, in the Data Protection Directive, it too was motivated by what had come to be called – particularly in Germany- the constitutional right to personal data protection.[32] This right was formally recognized, in 2000, by Article 8 of the European Charter of Fundamental Rights. An integral part of the early regulation of digital markets was the creation of privacy DPAs with regulatory, oversight, and enforcement powers over public and private organizations that collected and used personal data. As the technology has advanced and new forms of digitalization have emerged, the response has been new laws and new overseers of fundamental rights, i.e. the Digital Services Act, which requires dedicated authorities for illegal content flagged by users of social media; and the Artificial Intelligence Act, with its national supervisory authorities.[33]

Turning to the issue of extraterritoriality, one of the constant aspects of European digital regulation has been the projection of the fundamental rights paradigm outside of national borders. The original Data Protection Directive was itself driven by the vigorous constitutional and ombudsman protection of data protection rights within a small subset of Member States which was then projected to the EU's other Member States.[34] Once the Directive was passed, its adequacy provisions created the legal grounds and mechanism for the transfer of data protection rights to third countries like the United States[35]. The general idea behind this model was that, consistent with the constitutional character of the Directive, every individual in the EU has a right to continuous protection of personal data, even in the event of transfers to third countries[36]. Under Article 25 of the Directive, in particular, data transfers were permitted only if the third country ensured an "adequate level" of data protection. If the third country did not guarantee an adequate level of data protection (and it is worth emphasizing that the adequacy assessment extends to the entire law of the third country), the transfer had to be blocked or was required to proceed via one of the channels set down in the Directive.

The Directive's extraterritorial effect was also expanded by the case law of the Court of Justice. The concerns raised by the a-territorial character of the internet and the market power of US-based platforms, bringing the *de facto* expansion of the US laissez-faire model, led the CJEU to extend considerably the territorial scope of application of the Data Protection Directive. In the famous *Google Spain* decision[37], the Court opted for a broad and flexible meaning of the notion of "establishment" (art. 4(1)(a) of the Directive 95/46/EC), which included data processing carried out by foreign operators with servers located outside of the EU.[38] Such interpretation appears consistent with the (itself not uncontroversial) "effects doctrine" of international law, according to which States may assert jurisdiction over acts committed abroad when these acts have effects in the territory of the regulating state, [39] and with the CJEU case law on competition law.[40] It has left an enduring mark on the architecture of EU data protection law. Article 3 of the GDPR follows the *Google Spain* ruling and expressly codifies the criterion of "targeting" as a factor triggering the application of the Regulation, laying the groundwork for a significant expansion of the territorial scope of the EU data protection model.[41] The impact of this mechanism has been substantial, including in the enforcement of data subject rights, namely the right to be delisted from search engine results.[42] When European citizens started to ask DPAs for global injunctions against Google and other digital platforms (with some success) the CJEU felt the need to limit the reach of EU remedies to the European digital sphere, in order to comply with international comity obligations.[43]

The synergy between Article 3 and the provisions on the outbound transfer of personal data (Articles 44 to 55 of the GDPR), has been the engine for extraterritorial transfer in multiple ways: (1) scope provisions, namely the one at issue in the *Google Spain* case, apply as long as services are offered in the EU; (2) international agreements, including most recently the US-EU Data Privacy Framework, which build data protection rights into the law and regulation of foreign jurisdictions; (3) the business practices of multinational corporations which, in the course of complying with EU law, adapt all of their operations to the European standard, even those segments that have no European connection, i.e. the Brussels Effect. Furthermore, the US's extraterritorial approach to national security (FISA Section 702) and law enforcement (CLOUD Act) led the European Parliament to amend the original GDPR proposal by voting a so-called anti-FISA clause in Article 48. This provision aims to limit the transfer of personal data to third-country public authorities even when such transfers are authorized or mandated by a decision of a foreign court, tribunal, or administrative authority.

As noted above, the rationale underpinning the entire legal framework is the continuous protection of the fundamental right to data protection. The easier the violations made possible by digital technologies, the stronger the pressures exerted by foreign governments through their e-surveillance programs, the tougher the reactions deployed, in terms of territorial extension, by EU law.

The EU's digital rules aimed at rights abuses on social media platforms also promise to have extraterritorial effects. The Digital Services Act (DSA), which draws on the experience of the earlier, voluntary Code of Conduct entered into between the EU and Facebook, Microsoft, Twitter and YouTube in May 2016, [44] requires that big platforms such as Facebook and X engage in extensive content moderation to address harms such as racist speech and defamation.[45] Many believe that content moderation, like data protection, will carry over into the operations of platform companies in the United States and other jurisdictions.[46] Indeed, Article 2 (1) of the DSA enshrines the 'targeting' criterion, similarly to the GDPR. It provides that the Regulation "shall apply to intermediary services offered to recipients of the service that have their place of establishment or are located in the Union, irrespective of where the providers of those intermediary services have their place of establishment".

The most recent developments suggest that the EU is taking an ever more assertive approach to extraterritoriality, driven this time around not only by fundamental rights but also by a new industrial policy of strategic autonomy and digital sovereignty. In 2020, soon after Ursula Von der Leyen became President of the EU Commission, the Commission announced a far-reaching digital package. It was comprised, among other texts, of two regulations on data use (Data Act) and data sharing (Data Governance Act), and, relatedly, the AI Act.

One of the most important policy documents issued by the Commission in the context of the digital package was the Communication "European Strategy for Data" .[47] This marks a watershed moment in the development of European digital regulation. Starting from the assumption that access to data is critical for the development of the digital economy, the Commission points out various weaknesses in the existing European approach, most importantly the insufficient volume of data sharing. Also, in the Commission's view both the economic and fundamental rights flaws with the current European approach are related to the fact that a "small number of Big Tech firms hold a large part of the world's data". [48] Furthermore, they control a disproportionate fraction of cloud services, which is the vital technological infrastructure for data flows. These digital oligopolies are almost entirely non-EU actors. A strong competitive gap is

therefore apparent and the "incentives for data-driven businesses to emerge, grow and innovate in the EU today" [49] are very low. Therefore, the main goal of the European data strategy is to create a regulatory infrastructure aimed internally at reducing the barriers to data sharing and externally at preventing foreign operators from unilaterally appropriating the value of European data. Control over data, both of a personal and non-personal nature, is therefore regarded as an essential component of Europe's digital sovereignty.[50] It is not surprising that in this scenario the rules on cross-border data flows and the territorial scope of the digital regulations assume critical importance.[51]

The call for a more assertive approach to territorial scope affected the actual shape of the most recent regulations on data and artificial intelligence. To begin with the AI Act, Article 2 provides for a territorial scope of application of that is unprecedented. The Regulation applies not only to (a) suppliers placing on the market or putting into service AI systems in the Union, and to (b) users of AI systems located in the Union, but also to (c) suppliers and users of AI systems located in a third country, when the output produced by the system is used in the Union. It is clear that such a solution is not only driven by the logic of fundamental rights[52] but also by an increasing concern for strategic autonomy and digital sovereignty[53].

Moving to the regulation of non-personal data, the turn towards digital sovereignty is even more apparent. The Data Act (on data use) opts for a broad territorial scope, accepting targeting as a sufficient criterion to trigger the application of the regulatory scheme (art. 1 (3) Data Act).[54] Furthermore, both the Data Governance Act (on data sharing) and the Data Act (on data use) extend the restrictions on outwards transfer of personal data to certain categories of non-personal data, thereby introducing a soft but effective form of data localization[55]. As a result, the obstacles to international data flows have been raised significantly and the EU is increasingly depicted as a "soft data localization actor". [56] To the extent that third-country transfers will continue to be possible in the future, the EU is accused of "digital colonialism" .[57] In particular, Article 5 (9) DGA sets out a mechanism similar to the GDPR, attributing to the Commission the power to declare that a third country affords an "essentially equivalent" protection of trade secrets and IP rights, that such protection is being effectively enforced and applied, and that effective judicial redress is available. In the absence of such declaration, data obtained for reuse cannot be transferred unless the re-user undertakes to comply with the obligations to protect IP and trade secrets, even after the data is transferred to the third country, and to accept the jurisdiction of the relevant Member State (art. 5 (10) DGA). Furthermore, with regard to certain non-personal data declared "highly sensitive", the Commission is empowered to adopt delegated acts supplementing the DGA by laying down special conditions applicable for transfers to third-countries; such conditions "may include terms applicable for the transfer or technical arrangements in this regard, limitations as regards the re-use of data in third-countries or categories of persons which are entitled to transfer such data to third countries or, in exceptional cases, restrictions as regards transfers to third-countries" (art. 5 (11) DGA). Similarly, Article 32 of the Data Act lays down an obligation for providers of data processing services to "Providers of data processing services shall take all adequate technical, organizational and legal measures, including contracts, in order to prevent international and third country governmental access and transfer of non-personal data held in the Union where such transfer or access would create a conflict with Union law or with the national law of the relevant Member State".

Quite interestingly, the logic behind the anti-FISA clause of the GDPR (art. 48) has been replicated in the Data Governance Act and the Data Act. As made clear by the Commission in the

Impact Assessment Report accompanying the Data Act,[58] it is feared that foreign authorities may unlawfully access non-personal data stored in the cloud environment. Not unlike what happened to personal data in the *Microsoft Ireland* case, the risk is that cloud providers will be required by foreign courts or administrative authorities to hand over data processed in Europe. The Commission specifically refers to the US President's Executive Order 12333, FISA Section 702, the CLOUD Act, and the 2017 National Intelligence Law (China).[59] Commercially sensitive data appear particularly vulnerable in this regard. European firms may be discouraged from using cloud services in the absence of a protective framework, with the unfortunate consequence of "[restraining] the full potential of the data economy in Europe". [60] Consequently, Article 31 DGA and Article 32 (2) Data Act state that third-country courts or administrative authorities may not compel beneficiaries of the right to re-use data or data intermediation services providers to transfer or give access to non-personal data falling within the scope of such Regulations in the absence of an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union. Exceptionally, a transfer may be admissible if it is demonstrated that the third-country system requires the reasons and proportionality of the decision or judgement to be set out, the decisions are specific in character, any possible objection of the addressee is subject to a review by a competent court, and this court is empowered to take into account the relevant legal interests of the provider of the data protected by Union law or national law of the relevant Member State.[61] The Data Act entrusts the European Data Innovation Board with the task of advising and assisting the Commission in developing guidelines on the assessment of whether these conditions are met (art. 32 (3)).

The regulatory tools deployed in the new digital package unveil a growing concern for data control as a particular component of digital sovereignty. Arguably they will limit, or at least make more complicated, cross-border data flows. As happened in the field of personal data, the costs of compliance for international operators will be raised, and it might be that foreign governments come under increasing pressure to afford same the level of protection for non-personal data as afforded in the EU with the aim of obtaining a 'green card' from the Commission, i.e. an adequacy decision. This seems to be the bet behind the digital package: to gain the first-mover advantage and trigger a process of regulatory emulation abroad similar to what occurred with respect to personal data regulation.

Yet it is far from certain that the Brussels Effect will be replicated in the new digital context. To being with, the relative importance of the EU in the global economy is expected to diminish in the next future. More importantly, technical standards have become increasingly important in digital harmonization strategies, and the EU seems to have a weaker grasp on standardization processes (as shown by the rather unsuccessful experience with the cloud federation project Gaia-X). In addition, the EU's growing emphasis on strategic autonomy and increasing its share of the data economy may reduce the EU's credibility as a trade partner. Traditionally, the EU has been a supporter of openness in digital relationships and has been critical in international fora of data-localization requirements. [62] But times have changed. As argued by Andrea Renda, there is the risk that "while trying to introduce measures that counter-balance the power of non-EU technology giants, the EU ends up introducing digital trade barriers for developing countries and adopting a counter-productive, quasi-autarchic approach to technology policy". [63] In any event, it seems undisputable that the new legislative trend unveils a rationale for the territorial extension of EU law which is significantly different from the one behind the GDPR. It can no longer be framed as part of a virtuous and altruistic narrative of

fundamental rights and it brings to the fore the more pragmatic and less gentle side of the EU's institutional experiment. It remains to be seen whether this paradigm shift will prove effective in practice and will succeed in overcoming the internal contradictions that affect the new digital regulatory package of the EU.

IV. CHINA

We argued at the outset that the way in which law regulates digital innovation differs dramatically around the globe. We contrasted two main paradigms - the American ballot-box democracy and the European fundamental rights approach – and we explored the implications of such paradigms for the specific issue of 'extraterritoriality'. The picture would be incomplete if the third main player in the field, China, were not taken into account.

The broad-brush differences between the Western and the Chinese models of market regulation are well known and have been scrutinized by a copious comparative law literature.[64] Many argue that market regulation in China and other authoritarian regimes follows a "rule by law" paradigm.[65] Judicial review of administrative agencies, local authorities, and other types of government actors is primarily designed to ensure that the government stays within the four corners of the laws. Rule by law is very different from the traditional rule of law liberalism of the nineteenth and twentieth centuries, in which judicial policing of the limits of the law is conceived as a device for guaranteeing individual liberty from arbitrary government action. In the rule by law paradigm, the rules and their enforcement by courts operate as a mode of central government control over the sprawling bureaucracy and local governments. Rules and judicial enforcement of the rules, as hypothesized by the proponents of this model, also serve to signal to outsiders that the domestic market is safe for foreign investment and other types of market activity. At the time it was hypothesized, there was a hope that the rule *by* law would eventually morph into rule *of* law—that courts would indeed become independent and that by policing the limits of the law they would safeguard individual liberty against arbitrary government action.

Whether, even at the time it was proposed, the rule by law paradigm captured Chinese theories of how markets should be regulated is an open question. Today, however, the overwhelming power of the Chinese Communist Party and the authoritarian politics of all branches of government casts doubt on the ability of courts to reliably enforce rules. Moreover, specifically with respect to the internet, the nature of the market and the state interests involved suggest that the rule by law paradigm does not have much purchase over regulation of the digital sector.[66] Market power is concentrated among relatively few actors and therefore it is possible for central government ministries to regulate directly, without involving local government and other types of actors that might be hard to control from the center. In addition, the digital sector has been conceptualized as vital both to national security, through the prism of cybersecurity, and to authoritarian control over civil society, through censorship, and therefore the Communist Party has reasons to directly control the sector, using highly discretionary policies if necessary, without resorting to rules and courts for governance.

In China, what appears to be emerging is a layered approach to digital governance. At the deepest level is bureaucratic control of digital infrastructure, industry actors, and civil society users. Layered on top, however, there appears to be an attempt to improve the position of individuals through both digital platform regulation and competition law applied to the largest oligopolies (originally tolerated by the ruling party as part of a mercantilist policy aimed at supporting tech-innovation). We are witnessing, in other words, a gradual shift towards a model

of regulation in which a authoritarian state controls the essentials of the digital landscape (and can, unpredictably and arbitrarily intervene if things get out of control) but also seeks to create market spaces in which there is greater equality between consumers, on the one hand, and digital giants on the other. These new market spaces have been the object of recent laws which create the conditions for greater fairness and redistribution of digital platform economic power, as well as enhanced protection of Chinese citizens' privacy rights. To put it somewhat differently, due to the changing economic and social context, China is pragmatically embracing an approach that bears similarities with the European one but also continues to be strongly marked by "Chinese characteristics".

Early on, internet policy sought to achieve two main objectives: on the one hand boosting technological progress as a lever of economic growth and as a source of power in international relations; on the other hand, strengthening security and social stability in light of the risks ensuing from an uncontrolled internet. One should not underestimate the "American" roots of the extraordinary Chinese technological boom. It is true that start-ups were favored and subsidized in various ways by the government, but it is also undeniable that capital and knowledge flew in mass from the West (Goldman Sachs and other funds invested heavily in the new Chinese tech firms) and that a Silicon-Valley style of venture capitalism was replicated with great success in China.[67] In this phase, the Chinese state saw clearly the enormous advantages that could be gained, both externally and internally, from an increased access to the data collected by the platforms and from emerging AI technologies. Particularly under the Presidency of Xi Jinping, leadership in digital technologies came to be regarded as a strategic priority. The National Big Data Strategy was announced by the Central Committee of the Communist Party of China as part of its 13th Five-Year Plan in 2016; the New Generation Artificial Intelligence Development Plan was launched in 2017, with the explicit aim of making China the world leader in AI by 2030.[68]

Much effort has been devoted to the experimentation of controversial forms of e-governance, which are aimed at strengthening both social control and the economic competitiveness of the country.[69] While military and economic concerns were at the core of the AI strategy, social governance was equally important, given the challenges faced by a country living through such a sudden and intense transformation. The famous Social Credit program reflects such concerns[70]. As made clear by the 2014 State Council's Notice,[71] the main purposes of the Social Credit System are twofold: a) strengthening trust and accountability in commercial relationships as a tool of market expansion; b) discouraging anti-social behaviours and building an "harmonious" society along the lines of the core "socialist values". At the same time, the security of networks, data, and information has always been one of the absolute priorities of the Chinese government.[72] The Great Firewall project started at the beginning of the 2000s. The State Security Law was amended in 2015, to include the protection of core technologies and the infrastructure of network, information and data in sensitive fields (art. 25). In 2016, the Cybersecurity Law was enacted, detailing the state's task of enhancing data and network security, data localization requirements (art. 37), and the protection of critical information infrastructures.[73] New and more specific provisions were introduced in 2021, with the Data Security Law, a comprehensive state act that creates a new legal framework for cross-border transfer that will be detailed below.[74] A wide gamut of implementing regulations have followed.

Security and censorship, therefore, are constant traits of Chinese digital regulation. In recent times, however, there have been significant developments that have brought China – of course, only in certain aspects- closer to Europe. With the rise of the digital economy and the

pervasiveness of digital tools in mediating the daily life of most Chinese citizens (at least those living in cities), the need was felt to raise trust in digital platforms, enhance consumer protection and privacy rights, and curb the unfair business practices of large tech companies.[75] The Chinese state both deployed new legislative tools rooted in a private law logic and resorted to the regulatory and criminal instruments of antitrust investigations and criminal prosecution.

On the private law front, the rapidity which the right to privacy and data protection has been incorporated into Chinese law is impressive—even though it is at odds with many aspects of the Confucian tradition. The trajectory began with the Supreme People's Court judicial interpretation in 2001, followed by the Tort Law of 2009 (art. 2), which openly guaranteed privacy as an independent right.[76] Similarly, the Consumer Protection Act of 2013 stated that in B2C relationships, dignity and personal information shall be protected. The right to privacy was enshrined in Article 110 of the new General Rules of the Civil Law of 2017; also, Article 111 provides that "natural persons' personal information shall be protected by law". [77] Now, the completely new Civil Code adopted in May 2020 devotes an entire book (Book IV, divided into 6 Chapters) to personality rights.[78] To our knowledge, the Chinese Civil Code is the first in the world to do so. Technological innovation is specifically considered in various provisions of the Code, such as Article 1019 on the obligations deriving from information technology and defacing and imitating a person's own likeness.[79] Above all, the right to privacy and the right to personal information are extensively regulated (arts. 1032-1039), and specific guarantees are introduced in the field of credit rating and information to be provided to defaulters (arts. 1029-1030). Since the introduction of the right to privacy in Chinese law, litigation has skyrocketed and many claimants have successfully recovered damages in court.[80]

In 2021, the Personal Information Protection Law (PIPL) was also introduced. This is the first general regulation concerning data protection in China. It is strongly influenced by the EU GDPR and unambiguously recognizes in Article 2 that "the personal information of natural persons shall be protected by law. No organization or individual may infringe upon natural persons' rights and interests on their personal information". The PIPL applies to data processing both by public authorities and by private parties. However, consistent with the primacy accorded to state interests as articulated in specific administrative regulations or umbrella provisions (such as the public security exception in Article 26, which allows for unfettered video-surveillance), the PIPL's major impact is expected in private-to-private and particularly B2C relationships. Obviously, it is a law with Chinese characteristics. For instance, in contrast with Europe, supervision and enforcement is not entrusted to an independent administrative authority. But one should not underestimate its importance for the protection of data subjects and for overcoming the anarchic model of personal data collection and processing that characterized the first stage of the Chinese technological boom.[81]

On the regulatory and criminal front, in the early 2020s, the government started to resort aggressively to antitrust actions and at times also criminal prosecutions to weaken the market power of large tech companies and to incentivize them to adhere to government internet policy.[82] "Limiting the disorderly expansion of capital", in Xi Jinping's words, became a new priority. In 2021, Alibaba and Meituan were fined RMB 18.228 billion and RMB 3.442 billion respectively for antitrust violations; the merger of Huya and Douyu was suspended; several other platforms have received administrative penalties. In 2022, the Anti-Monopoly Law was amended to include the monopoly conduct of digital platforms. According to Article 9: "An undertaking shall not engage in any monopolistic conduct prohibited by this Law by utilizing data and algorithm,

technology, capital advantage, or platform rules, among others". Further regulations were adopted concerning more specific aspects of digital services; particularly noteworthy is the 2021 regulation on recommendation algorithms.

All these measures unveil a larger project of creating a layered digital economy. At the deepest level is a dense network of rules and principles consistent with the Weltanschauung of the ruling power and with the organizational forms of socialist legality. Embedded in this framework, however, is an attempt to create an orderly space of B2C digital relations. In this space, on specific issues such as cybersecurity responses, algorithmic fairness, consumer privacy, and limitations on market power, there are notable similarities to the European regulatory model.[83] Vice versa, the recent European attempt to fashion a concerted digital policy that promotes economic prosperity and digital sovereignty bears a certain resemblance to China's strategic mobilization of digital technologies.

The topic of extraterritoriality offers a clear example of the ongoing hybridization of the digital regulatory models. Initially, the Chinese Communist Party sought to advance its policy agenda through digital isolation but in recent years it has become clear to the Party that both the state and the B2C layers of its regulatory approach require that they be projected extraterritorially. In the early 2010s, China put in place the world's most rigid and comprehensive system of data localization, which worked as an essential tool to 're-territorialize' cyberspace and enforce Chinese digital authoritarianism.[84] As originally conceived, the data localization model was designed to protect Chinese interests and was defended in international fora by invoking the shield of territorial sovereignty.[85] Due to technological imbalances and the unbridled capacity of foreign corporations to collect and process data of their clients or contractors in China, the government sought to preserve control over Chinese data by requiring data storage on local servers and banning outbound transfers unless a prior administrative authorization was obtained.[86] These duties were set down in Article 37 of the Cybersecurity Law:

> Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and informatization departments and the relevant departments of the State Council to conduct a security assessment; where laws and administrative regulations provide otherwise, follow those provisions.

Since the Cybersecurity Law was first enacted, however, the global market share of Chinese tech companies has expanded significantly, and the economic downside of the rigid control of dataflows (particularly in the private sector) has been apparent. As a result, the original system of strict data localization has been loosened.[87] In a parallel trend, there has been a gradual shift from territorial sovereignty to functional extraterritoriality.[88] The 2021 Personal Information Protection Law and the 2021 Data Security Law offer clear hints of both tendencies: from a strict prohibition to conditional authorization of outbound data transfers; and from orthodox territoriality to the spatial expansion of China's digital sovereignty.

With respect to data localization, Article 38 of the Personal Information Protection Law (PIPL) is more flexible than the original mechanism contained in the Cybersecurity Law (now

replicated in art. 40 PIPL). Beyond the universal obligation to ensure an equivalent standard of protection abroad, obtain consent of the data subject, and provide a risk assessment, Article 38 offers four different avenues for any personal information processor who “truly needs to provide personal information for a party outside the territory of the People's Republic of China for business sake or other reasons”. The four legal avenues are the following: a) passing a security assessment organized by the State cybersecurity and informatization department; b) obtaining personal information protection certification conducted by a specialized body; c) concluding an agreement with a foreign receiving party according to the standard contract formulated by the State cybersecurity and informatization departments; or d) other conditions provided by the State cybersecurity and informatization department in laws or administrative regulations.

At the same time, US national security and law enforcement powers have left their marks on Chinese law, as they have on EU law. Article 41 PIPL introduces an anti-FISA clause that echoes Article 48 of the GDPR. It provides as follows:

> The competent authorities of the People's Republic of China shall handle foreign judicial or law enforcement authorities' requests for personal information stored within China in accordance with relevant laws and the international treaties and agreements concluded or acceded to by the People's Republic of China, or under the principle of equality and reciprocity. Without the approval of the competent authorities of the People's Republic of China, no organization or individual shall provide data stored in the territory of the People's Republic of China for any foreign judicial or law enforcement authority.

In the same vein, Article 36 of the Data Security Law provides that:

> the competent organs of the PRC are to handle requests for the provision of data from foreign justice or law enforcement based on relevant laws and international treaties and agreements concluded or participated in by the PRC, or in accordance with the principle of reciprocity. Domestic organizations and individuals must not provide data stored within the PRC to foreign justice or law enforcement bodies without the permission of the competent organs of the PRC.

With respect to functional extraterritoriality, both laws opt for a significant expansion of territorial scope.[89] By combining the territoriality principle and the effects doctrine, they promote “territorial extension,” a legal technique originally identified (in the EU context) by Joanne Scott.[90] Article 3, paragraph 2 of the PIPL stipulates the extraterritorial effect of its provisions:

> this Law shall also apply to the processing outside the territory of the People's Republic of China of the personal information of natural persons within the territory of the People's Republic of China, under any of the following circumstances: (1) for the purpose of providing products or services for natural persons inside the People's Republic of China; (2) analyzing or evaluating the behaviors of natural persons within the territory of the People's Republic of China; and (3) any other circumstance as provided by any law or administrative regulation.

Article 42 of the PIPL goes further by entrusting the national cyberspace department with developing a black list of overseas organizations or individuals engaging in personal information processing activities that “infringe upon the rights and interests of citizens of the People's

Republic of China on personal information or endanger the national security or public interests of the People's Republic of China". Transfers to such entities are prohibited and the list may be publicized and restrictive measures may be taken against Chinese companies. Similarly, Article 2 of the Data Security Law provides that

> data handling activities carried out outside the [mainland] territory of the P.R.C. that harm the national security of the P.R.C., the public interest, or the lawful rights and interests of citizens and organizations, are to be pursued for legal responsibility in accordance with law.

This new, bureaucratically managed window to the digital outside world has brought with it the principle of reciprocity. Reciprocity and multilateralims are invoked in several Chinese policy documents as the cornerstone of international data policy. Particularly noteworthy are the 2022 *Opinions of the CCP Central Committee and the State Council on Constructing a Basic System for Data and Putting Data Factors of Production to Better Use*[91], which insist on the importance of achieving a safe, compliant and orderly flow of data "in both directions across borders", improving the multi-sectoral coordination and cooperation-based system for cross-border data flow supervision, and at the same time opposing "data hegemony and data protectionism, and respond effectively to 'long-arm jurisdiction' in data fields" (par 11, page 8).

CONCLUSION

At the risk of wildly oversimplifying, this overview of regulatory models indicates three distinct approaches to digital governance: in the American model, the state piggybacks off the private sector; in the Chinese model, the private sector piggybacks off the state; and in the European model the state and private sector are mutually dependent, with the private sector traditionally shaped by extensive public protection for fundamental rights and, today, with the state sector increasingly getting into the business of making digital markets. Their approaches to extraterritoriality have tracked these different regulatory models: the extraterritorial projection of US interests through the global reach of Silicon Valley; in China, first data localization, and, now, a bureaucratically controlled form of extraterritorial engagement; and, in Europe, fundamental rights extraterritoriality together with an emerging preference for some data localization to promote both fundamental rights *and* economic and security interests.

Of these models, the American one appears to be the most static, if only because of the gridlock that marks the political system and the seeming impossibility of enacting federal legislation in the US Congress. By contrast, digital governance in both China and the European Union have undergone extensive transformation over the past decade and their models have come to share a certain resemblance. The question of how successfully these different jurisdictions will navigate the digital challenges on the horizon is an open one. To reframe the issue as one of digital constitutionalism, how will these different jurisdictions come to define the morally correct relationship between society and technology? And, in the future, will it be possible, from a comparative perspective, to keep learning by engaging with the world's legal systems, or will one model of digital governance prevail?

[1] See, e.g., Restatement (Fourth) of Foreign Relations Law § 404 (2018).
[2] See Julie R. O'Sullivan, 'The Extraterritorial Application of Federal Criminal Statutes: Analytical Roadmap, Normative Conclusions, and a Plea to Congress for Direction', *Georgetown Law Journal*, 106 (2018), 1034.
[3] Bignami, Francesca, 'A New Field: Comparative Law and Regulation', in Francesca Bignami and David Zaring, eds., *Comparative Law and Regulation: Understanding the Global Regulatory Process* (Cheltenham: Edward Elgar Publishing, 2016).
[4] See Carpenter v. U.S, 585 U.S. 296 (2018).
[5] HEW Report; May 1 version of S. 3418.
[6] See, e.g., Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.; the Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3402; the Video Privacy Protection Act, 18 U.S.C. § 2710; the Health Insurance Portability and Accountability Act, 110 Stat. 1936 (1996); the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.
[7] G. Trumbull, *Consumer Lending in France and America: Credit and Welfare* (New York: Cambridge University Press, 2014).
[8] U.S. v. Carolene Products Co., 304 U.S. 144, 152n. 4 (1938). The classic textbook identifies three primary rationales for today's First Amendment jurisprudence: information through the testing of ideas, democratic deliberation, and autonomy.
[9] Abrams v. U.S., 250 U.S 616, 630 (1919) (Holmes, J., dissenting).
[10] New York Times Co. v. Sullivan, 376 U.S. 254, 265 (1964).
[11] See Thomas E. Kadri & Kate Klonick, 'Facebook v. Sullivan: Public Figures and Newsworthiness in Online Speech', Southern California Law Review, 93/37 (2019).
[12] Kosseff, *Twenty-Six Words*, 95.
[13] Reno v. ACLU, 521 US 844 (1997).
[14] J. Kosseff, *The Twenty-Six Words That Created The Internet* (Ithaca: Cornell University Press, 2019), 3–4.
[15] Regulation 2016/679.
[16] Popkin, Helen A.S., 'Privacy Is Dead on Facebook. Get Over it.', NBC News (13 Jan. 2010), https://www.nbcnews.com/id/wbna34825225.
[17] Data Protection Directive, Articles 6 ["personal data must be . . . kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed."] 7, and 14).
[18] Daskal, Jennifer, 'The Opening Salvo: The CLOUD Act, e-Evidence Proposals, and EU-US Discussions Regarding Law Enforcement Access to Data Across Borders', in Francesca Bignami, ed., *EU Law in Populist Times* (New York: Cambridge University Press, 2020), 319.
[19] United States v. Microsoft, 138 S.Ct. 1186 (2018); Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E–Mail Account Controlled and Maintained by Microsoft Corp.) (*Microsoft Ireland*), 829 F.3d 197 (2d Cir. 2016), *reh'g denied*, Microsoft Corp. v. United States (*In re* Warrant to Search Certain E-Mail Account Controlled and Maintained by Microsoft Corp.), 855 F.3d 53 (2d Cir. 2017) (en banc).
[20] Stored Communications Act 18 U.S.C. §§2701-2713 (2018).
[21] Department of Justice, 'The Purpose and Impact of the CLOUD Act-FAQs', https://www.justice.gov/criminal-

oia/page/file/1153466/download#:~:text=The%20CLOUD%20Act%20clarified%20that,the%20company%20stores%20the%20data, accessed 3 Jan. 2024.
[22] United States v. United States District Court, 407 U.S. 297 (1972); Report on Foreign Intelligence Surveillance Act of 1978, 95th Congress, 2d Session, at 32.
[23] Bignami, Francesca, 'The US Legal System on Data Protection in the Field of Law Enforcement: Safeguards, Rights and Remedies for EU Citizens', European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE) (2015), https://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU%282015%29519215_EN.pdf, accessed 2 Jan. 2024.
[24] Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (Washington: PCLOB, 2023), https://documents.pclob.gov/prod/Documents/OversightReport/8ca320e5-01d3-4d6a-8106-3384aad6ff31/2023%20PCLOB%20702%20Report%20-%20Nov%2017%202023%20-%201446.pdf, accessed 11 Mar. 2024.
[25] Case C-362/14, Schrems v. Data Protection Comm'r, ECLI:EU:C:2015:650.
[26] Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions Issued by the U.S. Department of Commerce, annex I, 2000 O.J. (L 215) 7.
[27] Case C-362/14, Schrems v. Data Protection Comm'r, ECLI:EU:C:2015:650.
[28] Case C-311/18, Data Protection Comm'r v. Facebook Ireland, Maximillian Schrems, ECLI:EU:C:2020:559.
[29] Commission Implementing Decision EU 2032/1795 of 10 July 2023, Annex 1, 231 O.J.(L) 118; Sara Gerke & Delaram Rezaeikhonakdar, Privacy Shield 2.0—A New Trans-atlantic Data Privacy Framework Between the European Union and the United States, Cardozo Law Review 45/351 (2023).
[30] Bignami, Francesca, 'A New Field: Comparative Law and Regulation', in Francesca Bignami and David Zaring, eds., *Comparative Law and Regulation: Understanding the Global Regulatory Process* (Cheltenham: Edward Elgar Publishing, 2016), 18.
[31] Streinz, Thomas 'The Evolution of European Data Law', in Paul Craig and Gráinne de Búrca, eds., *The Evolution of EU Law* (Oxford: Oxford University Press, 2021), 902, 915.
[32] Council Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 L.J. (L281) 31; see generally Francesca Bignami, 'Cooperative Legalism', *American Journal of Comparative Law*, 59/2 (2011); A. Newman, *Protectors of Privacy* (Ithaca: Cornell University Press, 2008).
[33] Digital Services Act __; Data Governance Act, art. 29; AI Act, art. 59).

[34] A. Newman, *Privacy Regulators* (Ithaca: Cornell University Press, 2008); Francesca Bignami, 'Towards a Right to Privacy in Transnational Intelligence Networks', *Michigan Journal of International Law*, 28/3 (2007), 818.
[35] Dan J.B. Svantesson, 'Extraterritoriality in the Context of Data Privacy Regulation', *Masaryk University Journal of Law and Technology*, 7/1(2013), 87.
[36] T. Naef, *Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law* (Cham: Springer Nature, 2023), 55.
[37] CJEU, 13-5-2014, C-131/12, *Ag. Esp. Prot. Datos and Costeja Gonzalez v. Google Spain*; see also CJEU, Grand Chamber, 24-9-2019, C-507/17, *Google v. CNIL*.

[38] Brendan Van Alsenoy and Marieke Koekkoek, 'Internet and Jurisdiction after Google Spain: the Extraterritorial Reach of the "Right to be delisted"', *International Data Privacy Law*, 5/2 (2015), 105, 110–111; Claes G. Granmar, 'Global applicability of the GDPR in Context', *International Data Privacy Law*, 11/3 (2021).

[39] Adele Azzi, 'The Challenges Faced by the Extraterritorial Scope of the General Data Protection', *JIPITEC*, 9/2 (2018), 126, 131.

[40] Scott, Joanne, 'The Global Reach of EU Law', in Marise Cremona and Joanne Scott, eds., *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (Oxford: Oxford University Press, 2019), 36–38.

[41] Dan J.B. Svantesson, 'The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses', *Stanford Journal of International Law*, 50/1 (2014), 53.

[42] Quinn, John, 'Google v. CNIL: Circumscribing the Extraterritorial Effect of EU Data Protection Law', in Federico Fabbrini, Edoardo Celeste, and John Quinn, eds., *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Bloomsbury: Bloomsbury Publishing, 2021), 47, 50.

[43] CJEU, Grand Chamber, 24-9-2019, C-507/17, *Google v. CNIL*; see Stephan Kolo ßa, 'The GDPR's Extraterritorial Scope: Data Protection in the Context of International Law and Human Rights Law', *ZaöRV* 80 (2020), 791, 797; Quinn, 'Google v. CNIL', 54–62.

[44] European Commission, 'Code of Conduct on Countering Illegal Hate Speech Online', https://commission.europa.eu/document/551c44da-baae-4692-9e7d-52d20c04e0e2_en, accessed 2 Jan. 2024.
[45] Regulation 2022/2065, OJ L 277, October 27, 2022.
[46] Dawn C. Nunziato, 'The Digital Services Act and the Brussels Effect on Platform Content Moderation', *Chicago Journal of International Law*, 24/1 (2023).
[47] EUROPEAN COMMISSION, *A European Strategy for Data*, COM(2020) 66 final, (Brussels: European Commission, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066.
[48] *A European Strategy for Data*, 3.
[49] *Ibid.*
[50] Celeste, Edoardo 'Digital Sovereignty in the EU: Challenges and Future Perspectives', in Federico Fabbrini, Edoardo Celeste, and John Quinn, eds., Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty (Oxford: Hart Publishing, 2021), 217.

[51] *A European Strategy for Data*, 23–24.
[52] Luciano Floridi, 'The European Legislation on AI: a Brief Analysis of its Philosophical Approach', *Philosophy and Technology*, 34 (2021), 216–217.
[53] Celeste, 'Digital Sovereignty in the EU: Challenges and Future Perspectives', 211.

[54] Art. 1 (3) provides as follows: "This Regulation applies to: (a) manufacturers of connected products placed on the market in the Union and providers of related services, irrespective of the place of establishment of those manufacturers and providers; (b) users in the Union of connected products or related services as referred to in point (a); (c) data holders, irrespective of their place

of establishment, that make data available to data recipients in the Union; (d) data recipients in the Union to whom data are made available; […] (f) providers of data processing services, irrespective of their place of establishment, providing such services to customers in the Union; […]".

[55] For a functional assessment of various data localization schemes, Ursic, Helena, et al., 'Data Localization Measures and Their Impacts on Data Science', in *Research Handbook in Data Science and Law* (Cheltenham: Edward Elgar, 2018), 322; see also Naef, *Data Protection without Data Protectionism*, 236.
[56] Elaine Fahey, *The EU as a Global Digital Actor: Institutionalising Global Data Protection, Trade, and Cybersecurity* (Bloomsbury Publishing: Bloomsbury, 2022), 39–45.
[57] S. Scasserra and C. M. Elebi, *Digital Colonialism: Analysis of Europe's Trade Agenda* (Amsterdam: Transnational Institute, 2021).
[58] Commission Staff Working Document, *Impact Assessment Report* accompanying the Data Act Proposal, SWD (2022) 34 final, at 20–21.
[59] *Impact Assessment Report*, 21, note 97.
[60] *Impact Assessment Report*, 21.
[61] Art. 32 (3) Data Act.
[62] The Commission has in various occasions denounced the foreign impediments against data flow and openly rejected any form of digital protectionism. For instance, in EUROPEAN COMMISSION, *Trade for All: Towards a More Responsible Trade and Investment Policy*, COM(2015) 497 final, (Brussels: European Commission, 2015), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0497, 7, the EU Commission noted that "European companies still face significant barriers around the world, such as non-transparent rules, government interference, unjustified data localisation and data storage requirements". Clearly, what counts as a "justified" reason for data localisation requirements is open to debate.
[63] Andrea Renda, 'Beyond the Brussels Effect: Leveraging Digital Regulation for Strategic Autonomy', *Foundation for European Progressive Studies*, (2022), 14.
[64] Bignami, Francesca, 'A New Field: Comparative Law and Regulation', in Francesca Bignami and David Zaring, eds., *Comparative Law and Regulation: Understanding the Global Regulatory Process* (Cheltenham: Edward Elgar Publishing, 2016); van Rooij, Benjamin, 'The Campaign Enforcement Style: Chinese Practice in Conext and Comparison', in Francesca Bignami and David Zaring, eds., *Comparative Law and Regulation: Understanding the Global Regulatory Process* (Cheltenham: Edward Elgar Publishing, 2016), 217–237; Huang, Cheng-Yi and Law, David S., 'Proportionality Review of Administrative Action in Japan, Korea, Taiwan, and China', in Francesca Bignami and David Zaring, eds., *Comparative Law and Regulation: Understanding the Global Regulatory Process* (Cheltenham: Edward Elgar Publishing, 2016), 305–334.
[65] Ginsburg, Tom and Moustafa, Tamir, 'Introduction: The Function of Courts in Authoritarian Politics', in Tom Ginsburg and Tamir Moustafa, eds., *Rule by Law: the Politics of Courts in Authoritarian Politics* (Cambridge: Cambridge University Press, 2008).
[66] Creemers, Rogier 'The Great Rectification: A New Paradigm for China's Online Platform Economy', Competition Policy International, (16 Jan. 2023), https://www.pymnts.com/cpi_posts/the-great-rectification-a-new-paradigm-for-chinas-online-platform-economy/.
[67] K.F. Lee, *AI Superpowers: China, Silicon Valley, and the New World Order* (Boston: Houghton Mifflin Harcourt, 2018), 51–103.

[68] Huw Roberts, et al., 'The Chinese Approach to Artificial Intelligence: An Analysis of Policy and Regulation', *AI and Society*, 36 (2021).
[69] P. Du, et al., *The Development of E-Governance in China* (Singapore: Springer Singapore, 2019).
[70] For an overview see Yu-Jie Chen, et al., ''Rule of Trust': The Power and Perils of China's Social Credit Megaproject', *Columbia Journal of Asian Law*, 32/1 (2018); Daithí Mac Síthig and Mathias Siems, 'The Chinese Social Credit System: A Model for Other Countries?', *EUI Working Papers*, 2019/01 (2019); Larry C. Backer, 'Next Generation Law: Data Driven Governance and Accountability Based Regulatory Systems in the West, and Social Credit Regimes in China', *Southern California Interdisciplinary Law Journal*, 28/1 (2019).
[71] 'Notice concerning Issuance of the Planning Outline for the Construction of the Social Credit System 2014-2020', *China Copyright and Media*, https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/, accessed 3 Jan. 2024.
[72] Rogier Creemers, 'Cybersecurity Law and Regulation in China: Securing the Smart State', *China Law and Society Review*, 6 (2021), 111; Ibid., Creemers, Rogier, 'The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy', Journal of Contemporary China, (30 March 2023), https://doi.org/10.1080/10670564.2023.2196508, accessed 3 Jan. 2024.

[73] Creemers, 'Cybersecurity Law and Regulation in China: Securing the Smart State', 118–121.
[74] Creemers, 'Cybersecurity Law and Regulation in China: Securing the Smart State', 122–123.
[75] Creeemers, Rogier, 'The Great Rectification: A New Paradigm for China's Online Platform Economy', (10 Jan. 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4320952.
[76] Chen Lei, 'Debating Personality Rights Protection in China: A Comparative Outlook', *European Review of Private Law*, 26/1 (2018), 31.
[77] See also the 2017 Cybersecurity Act (art. 21, 41–45, 76), creating an obligation for network operators to protect natural persons' and civil subjects' personal information; recently the General Administration of Quality Supervision and Standardization issued a (non-binding, but important) Personal Information Security Specification ("The Standard" 2018). Roberts, et al., 'The Chinese Approach to Artificial Intelligence: an Analysis of Policy and Regulation', 69–70.
[78] Liming Wang and Bingwan Xiong, 'Personality Rights in China's New Civil Code: A Response to Increasing Awareness of Rights in an Era of Evolving Technology', *Modern China*, 47/6 (2021), 703; Giorgio Resta, 'Codifying Personality Rights in China: Legacy of Tradition and Emerging Issues', paper presented at the Sino-European Conference on Chinese Civil Code, Beijing, 21–22 September 2019, on file with the author.
[79] Wang and Xiong, 'Personality Rights in China's New Civil Code: A Response to Increasing Awareness of Rights in an Era of Evolving Technology', 715.
[80] Ibid., 709; see also for a discussion of selected cases, Lei, 'Debating Personality Rights Protection in China: A Comparative Outlook', 45–49.
[81] Lee, *AI Superpowers: China, Silicon Valley, and the New World Order*, 55–56. Incidently, as Lee explains, this anarchic model explains China's impressive results in many fields of AI innovation.
[82] A. Bradford, *Digital Empires* (Oxford: Oxford University Press, 2023), 94; Creeemers, *The Great Rectification*.
[83] Creemers, 'Cybersecurity Law and Regulation in China: Securing the Smart State', 133.

[84] Carwyn Morris, ‘It Would be Smart to Discuss This on Telegram’: China’s Digital Territorialization Project and its Spatial Effects on Contentious Politics’, *Territory, Politics, Governance*, 11/6 (2023), 1081, 1085.
[85] Wang, Yukai, ‘Regulating Outbound Data Transfer: The Practice of China and a Comparative Approach’, in Marina Timoteo, Barbara Verri, and Riccardo Nanni, eds., *Quo Vadis, Sovereignty? New Conceptual and Regulatory Boundaries in the Age of Digital China* (Cham: Springer Cham, 2023), 169–180.
[86] Wang, ‘Regulating Outbound Data Transfer’, 174.
[87] Cong, Wanshu, ‘The Spatial Expansion of China's Digital Sovereignty: Extraterritoriality and Geopolitics’, (2 Sept. 2021), https://ssrn.com/abstract=4019797, accessed 3 Jan. 2024.
[88] Zhengxin Huo and Man Yip, ‘Extraterritoriality of Chinese Law: Myths, Realities and the Future’, *Chinese Journal of Comparative Law*, 9/3 (2021), 328.
[89] Cong, ‘Spatial Expansion of China's Digital Sovereignty’, par. 2.
[90] Scott, Joanne, ‘The Global Reach of EU Law’, in Marise Cremona and Joanne Scott, eds., *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (Oxford: Oxford University Press, 2019), 21.

[91] Center for Security and Emerging Technology, ‘Opinions of the CCP Central Committee and the State Council on Constructing a Basic System for Data and Putting Data Factors of Protection to Better Use’, https://cset.georgetown.edu/publication/opinions-of-the-ccp-central-committee-and-the-state-council-on-constructing-a-basic-system-for-data-and-putting-data-factors-of-production-to-better-use/, accessed 3 Jan. 2024.