Data protection as an emerging norm for cyberspace activities: two national approaches to balancing national security considerations with data privacy

Deborah Housen-Couriel

Keywords: data protection, data privacy, privacy rights, cyber privacy, GDPR, EU, China

Contents
1. Introduction to the concept of “cyber privacy” ............................................................... 2
2. Data privacy rights: a brief overview .............................................................................. 4
3. Balancing national security and data privacy rights ....................................................... 6
4. Two regulatory initiatives for personal data protection: the EU’s GDPR and China’s Cybersecurity Law ................................................................................................................. 8
   4.1 The EU’s General Data Protection Regulation ......................................................... 9
   4.2 China’s Cybersecurity Law ...................................................................................... 13
5. Comparisons and conclusions: towards a better understanding of “cyber privacy” ......... 21

Abstract: Data protection is emerging as an essential element of international cybersecurity and stability in cyberspace. Cybersecurity strategies, policies, and regulations increasingly include it as an inherent part of the advancement and achievement of national, regional and international cybersecurity goals. Moreover, this trend towards convergence of data protection and cybersecurity is underway in a diverse array of jurisdictions in the Western hemisphere, in Africa and in Asia. This development represents an important next phase in the governance of cyberspace at both the international and national levels, broadening the conceptual basis for government and organizational mitigation of cyberspace risks and threats. Especially given the present cyber threat landscape, partly characterized by hostile actors’ intensive exploitation of data vulnerabilities, it is critical for regulators and policymakers to move ahead with the integration of data protection regimes in cyberspace – or “cyber privacy” – with cybersecurity laws and regulations. The EU and China regulatory models (respectively, the General Data Protection Regulation (GDPR) and China’s Cybersecurity Law (CCL) draw global attention to the need for more robust and transparent balancing mechanisms between cybersecurity needs and privacy rights, ultimately contributing towards increased levels of cyber stability and security overall. The difficult challenge that lies ahead is the coordination at the regional and global levels of emerging cyber privacy regimes such as the GDPR and the CCL, in order to better leverage the regulatory tools that are becoming increasingly available for achieving this common aim.

1 The author acknowledges the generous research support undertaken by the Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University. I am indebted to Rogier Creemers for his helpful comments on the text. Responsibility for any errors is mine alone.
1. Introduction to the concept of “cyber privacy”

Data protection is emerging as an essential element of international cybersecurity and stability in cyberspace. Cybersecurity strategies, policies, and regulations increasingly include it as an inherent part of the advancement and achievement of national, regional and international cybersecurity goals. Moreover, this trend towards convergence of data protection and cybersecurity is underway in a diverse array of jurisdictions in the Western hemisphere, in Africa and in Asia.²

This development represents an important next phase in the governance of cyberspace at both the international and national levels, broadening the conceptual basis for government and organizational mitigation of cyberspace risks and threats.³ Especially given the present cyber threat landscape, partly characterized by hostile actors’ accelerated, even “catastrophic” exploitation of personal data and intellectual property vulnerabilities,⁴ it is critical for regulators and policymakers to move ahead with the integration of data protection regimes in cyberspace – or “cyber privacy” – with cybersecurity laws and regulations.⁵

There are two potentially significant outcomes for such a development. First, current conceptual gaps within national jurisdictions will be narrowed, as the new, broadened concept of cybersecurity will more clearly come to encompass personal data and intellectual property vulnerabilities. Secondly, cyber risks and their costs will be significantly re-distributed, since data protection regimes explicitly impose regulatory responsibility and accountability for vulnerabilities to corporations and individuals.

---


³ On the convergence of data protection and cybersecurity, see Schackelford, supra note 2. See also Jay P. Kesan & Carol M. Hayes, Creating a ‘Circle of Trust’ to Further Digital Privacy and Cybersecurity Goals, 2014 MICH. ST. L. REV. 1475 (2014).


⁵ Cyber privacy is not restricted to the Internet, as it relates to the protection of personal data through all parts of cyberspace: wi-fi, mobile telephony, and geolocation services in addition to communication via the internet.
Although these two outcomes may, at the first stage, influence only the domestic jurisdictions in which national laws have in fact integrated data protection and cybersecurity (including in the two jurisdictions studied herein below), they may eventually have a broader regional, and perhaps global impact.\(^6\) We return to a brief discussion of this concept in the conclusion below.

In this article, we focus on a single aspect of the concept of cyber privacy: the balancing of national security needs with individual data privacy rights. This inherent regulatory tension remains a core dilemma at the forefront of rule of law concerns in cyberspace.\(^7\) Recent regulatory initiatives to address the protection of individuals’ personal data in cyberspace on the part of two jurisdictions that are leading state actors in cyberspace, the European Union and China, serve as a reminder that this is a critical issue in cyberspace governance and cybersecurity, and that the stakes are high for determining the right balance. A third key jurisdiction, the United States, is ripe for reform of its data protection regime in the wake of multiple data breaches in 2017 and 2018 – unprecedented in scope – resulting in major financial and reputational losses,\(^8\) including the Equifax breach in which nearly half of U.S. citizens’ personal data was compromised.\(^9\) Recent legislation, the Clarifying Lawful Overseas Use of Data (CLOUD) Act,\(^10\) which addresses jurisdictional issues for data stored outside of U.S. sovereign territory, is an indicator that such reform is underway.\(^11\) Finally, a fourth major jurisdiction, India, is currently drafting a data protection law in the wake of a Supreme Court case in August 2017 that established a fundamental right to data privacy.\(^12\)


\(^7\) Compare G.A. Res. 69/166 of December 18, 2014 (recognizing the right to privacy in the digital age), with Human Rights Council, Res. 32/13, U.N. Doc. A/HRC/RES/32/13, art. 8 (July 18, 2016) (advancing the promotion, protection and enjoyment of human rights on the Internet, which “Calls upon all States to address security concerns on the Internet in accordance with their international human rights obligations to ensure protection of … privacy and other human rights online, including through national democratic, transparent institutions, based on the rule of law, in a way that ensures freedom and security on the Internet…”).


\(^10\) Clarifying Lawful Overseas Use of Data (CLOUD) Act, H.R. 4943, 115th Congress (2d Sess. 2018). Section 2713 states: “A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider’s possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.” (emphasis added).

\(^11\) The personal data protection regime under U.S. law is beyond the scope of the present article. For review and analysis of that regime see, for example, O’Connor, supra note 9.

\(^12\) Justice K.S. Puttaswamy (Retd) v. Union of India, (2014) 6 SCC 433 (India); White Paper of the Committee of Experts on a Data Protection Framework for India, (Dec. 18, 2017),
This article explores the emerging norms for data privacy, in the EU and China, both of which have recently promulgated binding norms – EU’s General Data Protection Regulation (GDPR)\textsuperscript{13} and China’s Cybersecurity Law (CCL)\textsuperscript{14} – to balance the protection of personal data privacy in cyberspace with security considerations. In China’s case, these considerations relate to national security; and in the EU, both member countries’ national security considerations and, due to the EU’s unique organizational structure, European regional security considerations. We propose that the balancing models put forward in the GDPR and the CCL provide interesting insights into how a more general understanding of the protection of personal data as an integral part of national and regional cybersecurity norms and regimes may be gleaned in other regulatory contexts. In particular, the rule of law limitations on government access to personal data within a given data privacy regime is implemented will, in our view, determine its ultimate effectiveness in protecting the individual’s right to data privacy.

2. Data privacy rights: a brief overview

Data privacy rights represent a special form of respect for the human right to privacy.\textsuperscript{15} An individual’s right to have his or her personal data – name, telephone number, address, health, physical location, biometric, financial information, and other identifiers\textsuperscript{16} – protected from use by others without consent is derived from the general right to individual privacy. This right to privacy has been codified at the international level by, \textit{inter alia}, the Universal Declaration of Human Rights (UDHR),\textsuperscript{17} the International Covenant on Civil and Political

\textsuperscript{13} Council Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119/1) [hereinafter GDPR].


\textsuperscript{16} While the types of personal data included in regulatory definitions of protected personal data vary from jurisdiction to jurisdiction, they generally include any piece of information that can conclusively identify the individual independently or by readily-available cross-referencing. See definitions below, infra notes 28 & 55.

\textsuperscript{17} G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948).
Rights (ICCPR), the European Convention for the Protection of Human Rights and Fundamental Freedoms, and a number of other regional human rights treaties. Article 17 of the ICCPR provides, for instance, that “arbitrary or unlawful interference” with an individual’s “privacy…or correspondence” is forbidden, and that there is a right to the protection of the law against such interference. UN bodies have also engaged with the implementation of data privacy rights in cyberspace: two leading examples are the 2014 UN General Assembly Resolution on the right to privacy in the digital age; and the 2016 UN Human Rights Council resolution on the promotion, protection and enjoyment of human rights on the Internet. The 2015 GGE Report of the Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security also emphasized that “…States should guarantee full respect for human rights, including privacy…”

Thus, data privacy rights have been formalized at the international level, notwithstanding the overall challenges to enforcement of such rights within domestic jurisdictions. Yet with half of the world’s population currently using the internet, the exponential increase in transborder data flows, including personal data, has brought many countries to the conclusion that the “…general reference to the right to privacy [is] no longer considered sufficient to protect

---

21 G.A. Res. 69/166, supra note 7.
22 Human Rights Council Res. 32/13, supra note 7. The thirteenth paragraph of the preamble recognizes that “…it is imperative that States address security concerns in accordance with their international human rights obligations, in particular with regard to freedom of expression, freedom of association and privacy.” Article 8 of the Resolution calls upon states to achieve this balance. See also Enoken Tikk-Ringas, Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012, ICT4Peace (2012); Tim Maurer, Cyber Norm Emergence at the United Nations, 36, 64 (Harvard Kennedy School Belfer Center, Discussion Paper 2011-11, 2011).
individual rights.24 Moreover, national and regional jurisdictions may interpret and apply data privacy rights in radically different ways.25

For instance, the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations notes that international human rights law applies to cyber-related activities of a state as a matter of lex lata,26 and that individuals enjoy the same international human rights (such as privacy) with respect to cyber-related activities.27 Yet the Manual emphasizes that the diverse contexts in which these rights are realized must be fully acknowledged in the cyber context:28

The [Group of Experts] agreed with the assertion that ‘the realisation of human rights must be considered in the regional and national context bearing in mind different political, economic legal, social, historical, and religious backgrounds’. This point is especially relevant in the cyber context given differing levels of cyber development, economic wherewithal, national and regional security concerns, and the like.29

This diversity of approach inherent to the substance of domestic law data privacy protections, as well as the rule of law context in which these protections are implemented, is a central point to which we will return throughout the analysis below and in the article’s conclusion.

In sum, we argue herein that data protection regimes on both the domestic and international planes are currently evolving in this new cyberspace context as inherent and critical aspects of national and global cybersecurity. As such, they aim to balance an array of rule of law challenges given the global, trans-jurisdictional nature of the flow of personal data.30

3. Balancing national security and data privacy rights

The balance of individual rights, such as privacy rights, with lawful national security needs in cyberspace presents a challenging regulatory task. As with other human rights codified in international instruments and domestic regulations, derogation from data privacy safeguards is usually permitted through carve-outs with respect to national security, public order, and

26 TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt & Liis Vihul eds., 2d ed. 2017) at 182.
27 Id. at 187-192.
28 Id. at 180.
29 Id. at 180 (citing Article 7 of the ASEAN Human Rights Declaration, Nov. 18, 2012, http://asean.org/asean-human-rights-declaration/ (emphasis added)).
30 Bygrave, Data Protection, supra note 15.
public welfare considerations. Additional conditions may include necessity and proportionality. However, when derogations are permitted, an important rule of law consideration is the existence of lawfulness criteria that curtail their scope. For example, UDHR Articles 29 (2) and (3) stipulate:

2. In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.

3. These rights and freedoms may in no case be exercised contrary to the purposes and principles of the United Nations.

Misuse and abuse of these criteria by governments is an ongoing concern. Specifically, with respect to data privacy rights, the UN Human Rights Council’s Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on the internet, Frank LaRue, emphasized this difficulty in his 2011 Report:

The Special Rapporteur is deeply concerned by actions taken by States against individuals communicating via the Internet, frequently justified broadly as being necessary to protect national security or to combat terrorism. While such ends can be legitimate under international human rights law, surveillance often takes place for political, rather than security reasons in an arbitrary and covert manner. [...] The necessity of adopting clear laws to protect personal data is further increased in the current information age, where large volumes of personal data are collected and stored by intermediaries, and there is a worrying trend of States obliging or pressuring these private actors to hand over information of their users. Moreover, with the increasing use of cloud-computing services, where information is stored on servers distributed in different geographical locations, ensuring that third parties also adhere to strict data protection guarantees is paramount.

For example, the UDHR permits derogations in Article 29 (2) and (3), and the European Convention for the Protection of Human Rights and Fundamental Freedoms permits derogations in Article 18 (with specific derogations in other articles). See Fidler, supra note 20, at 101.


See e.g., ICCPR, supra note 18, arts. 12, 14, 18, 19, 21, 22 & 23.

UDHR, supra note 17 (emphasis added).


The dilemma emphasized by LaRue is especially conspicuous in public debate on individual rights in cyberspace since the revelation of the U.S. government’s global surveillance practices by Edward Snowden in 2013. Yet regulators at the national, regional, and global levels have yet to fully engage with this dilemma and the protection of both national security and individual rights in cyberspace. Moreover, it represents a truly difficult balancing of key substantive issues in a rapidly-developing regulatory environment that needs to encompass new technological challenges on a regular basis. For instance, in recent years data privacy has required protection in the context of technological developments such as cloud computing services that inherently transcend national regulatory boundaries; the Internet of Things; and the widespread use of algorithms for automated profiling. All of these phenomena were in their infancy a decade ago. At the same time, exploitation of these same technologies for hostile and criminal cyber activities has become commonplace. Concerns are acute regarding security and law enforcement, prompting additional regulatory modes of personal data surveillance and retention on the part of governments, such as the controversial 2016 Investigatory Powers Act of the UK, portions of which have been found unconstitutional by UK courts. This “strange paradox” of the simultaneous strengthening and weakening of individual rights, such as data privacy in the cyberspace, has been noted by Viktor Schoenberger-Mayer and Teree Foster.

4. Two regulatory initiatives for personal data protection: the EU’s GDPR and China’s Cybersecurity Law

Two recent examples of domestic regulation, both promulgated in 2016, adopt models for balancing national security with the protection of personal data privacy in cyberspace that exhibit an interesting combination of converging modalities and diverging regulatory


40 Schoenberger-Mayer and Foster refer specifically to the regulation of free speech in cyberspace, although they include data privacy protection in the scope of their analysis. See Viktor Mayer-Schönberger & Teree Foster, A Regulatory Web: Free Speech and the Global Information Infrastructure, in BORDERS IN CYBERSPACE 235, 243 (Brian Kahin & Charles Nesson eds., 1999). See also Fidler, supra note 20, at 102.
approaches. The EU’s GDPR and China’s CCL both undertook this challenging regulatory task in the current dynamic and uncertain cybersecurity environment. The new regimes include updated and explicit data protection norms and measures that share similarities regarding the definition of protected data, data subject consent, notification of data breaches, the right to rectification of erroneous data, and other safeguards and modalities.

On the other hand, the approaches of EU and Chinese regulators to carving out exemptions for security and law enforcement requirements reflect radically different concepts of how this balance should be calibrated. Setting aside important disparities in both the nature of governance and the concept of the rule of law in these two regimes, some key highlights distinguish their regulatory strategies to resolve tension between personal data protection and national security, although a full comparative analysis is beyond the present scope. The analysis focuses on the “law on the books” rather than de facto implementation; those aspects relating to the implementation of these data protection regimes will also require additional research.

4.1 The EU’s General Data Protection Regulation

4.1.1 The data protection regime

The EU’s GDPR, entering into force on May 25, 2018, provides a leading example of emerging norms for regulatory protection of personal data privacy. Significantly, the GDPR is supported by robust administrative and civil enforcement measures that establish normative jurisdiction for data subject rights not only within EU territorial borders, but also outside of the EU. The operative provision is GDPR Article 3, entitled “Territorial scope”, which provides as follows:

42 GDPR, supra note 13.
43 CCL, supra note 14.
1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, {
regardless of whether the processing takes place in the Union or not.}

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
   a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
   b) the monitoring of their behaviour as far as their behaviour takes place within the Union […] 46

This ostensible “jurisdictional grab” has not escaped controversy and legal critique (one critic derided part of the GDPR enforcement regime as “privacy tourism”47), yet its actual trans-jurisdictional impact remains to be seen following the GDPR’s entry into force.48

So far, the EU has opted for a regulatory separation between its data protection regime under the GDPR and the overall context of EU cybersecurity, which was addressed in the 2016 Network Security Directive.49 This separation is not without consequences at the level of national legislation – which is mandated under EU directives, but not under EU regulations50 – nor at the enforcement level of data protection as an inherent and critical part of cybersecurity. In contrast, as shall be shown below, China made a different regulatory choice by folding its data protection regime into the broader scope of its Cybersecurity Law.

The personal data that is subject to the GDPR regime is defined broadly, as follows:

…any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;51

---


51 GDPR, supra note 13, art. 4.
Such personal data of EU residents is protected by extensive safeguards and may be processed exclusively within the bounds of legality set out in Article 6 of the GDPR. These legality bases include specific consent on the part of the data subject, performance of a contract between the data subject and the data controller, compliance with a legal obligation of the data controller, and a controller’s “legitimate interest.”

More amorphous situations exist under Article 6 (d) and (e), where (respectively) “processing is necessary in order to protect the vital interests of the data subject or of another natural person”; and “processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.” Processing of personal data may be carried out without data subject consent or knowledge under the broad scope of these provisions. The legislative intent behind them is shared in GDPR Recitals 46 and 50, which shed some light on situations in which they may apply:

Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

Furthermore, data subject consent is not required for processing personal data under Article 23, entitled “Restrictions.” This broad carve-out, separate from the bases of legality established in Article 6, includes two types of restrictions on GDPR principles and data subject rights that may be established under EU or member state legislative measures: closed restrictions and open-ended restrictions. First, the “closed” grounds for restricting data subject rights include:

- national and public security;
- defense;
- criminal law enforcement;
- judicial independence and proceedings;
- ethical breaches for regulated professions;
- enforcement of civil law claims.

The open-ended considerations, potentially subject to a more flexible interpretation, are:

---

52 Id. art. 6.
53 Id. art. 4. The definitions in Article 4 provide that a “controller” determines “the purposes and means of the processing of personal data,” while a “processor” carries out the actual data processing.
54 GDPR, supra note 13, Recital 46.
55 Id. art. 23 (a), (b), (c), (d), (f), (g), (j).
important objectives of general public interest, such as economic, financial, public health and social security objectives;

- monitoring, inspection or regulatory functions connected to the exercise of official functions, even occasionally;
- the protection of the data subject or the rights and freedoms of others.\(^{56}\)

Thus, the GDPR permits derogation from its data protection regime with respect to broad categories of personal data processing.\(^{57}\)

In this respect, national security and law enforcement considerations have been clearly established by the EU regulator as outweighing data protection considerations. The overall presumption in favor of a fundamental right to data privacy is thus recalibrated when such factors are determined by national and EU regulators. As if to emphasize the intractability of the national security-privacy dilemma, on the same day the GDPR was promulgated, and immediately following its text in the EU’s *Official Journal*, two additional regulatory measures were adopted that carve out specific exceptions to GDPR personal data protections: one on the use of personal data for law enforcement, and the other on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.\(^{58}\)

Given the wide scope of these exemptions and carve-outs for national security and other considerations, questions arise as to the ultimate impact of the GDPR’s protection of data privacy rights on behalf of the data subject. Specifically, whether contemporary data regimes – even an assertive regime such as the GDPR premised on individual data privacy as a fundamental human right – are inevitably limited by security and law enforcement considerations, given present cybersecurity threat vectors.

### 4.1.2 Rule of law constraints

Significantly, the GDPR incorporates a specific set of constraints within its “exemptions regime,” setting out permissible limitations on the fundamental right of individual data privacy. These rule of law limitations are critical: while they echo the requirements limiting privacy in human rights treaties on necessity and proportionality grounds, they also go further in relying upon specific safeguards. Thus, lawful processing under Article 6 that does not rely

\(^{56}\) *Id.* art. 23 (e), (h), (i).

\(^{57}\) *Id.* art. 23.

upon data subject consent must be based in EU or member state law that meets “an objective of public interest and be proportionate to the legitimate aim pursued” and must be “fair.” Article 23 restrictions must also “[respect] the essence of the fundamental rights and freedoms and [constitute] a necessary and proportionate measure in a democratic society.” The EU or member state law establishing the basis for such restrictions must, to the extent possible, set out the specific provisions listed in Article 23 (2), such as purposes of processing, categories of data treated, and safeguards to prevent abuse. Recital 73 elaborates upon the intent:

Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters[…] the safeguarding against and the prevention of threats to public security, or […] other important objectives of general public interest …

These criteria may serve as a circumscribed basis for judicial interpretation of the permitted scope of exceptions to the GDPR personal data protections, following the GDPR’s entry into force. Moreover, GDPR Recital 73 concludes by stating that any restrictions on data subject rights “…should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.” On the one hand, these restrictive, rule of law provisions represent a positive development within the GDPR, showing regulatory restraint and a pro-active approach to ensuring individual rights for EU data subjects. On the other hand, the carve-outs may prove to eventually empty the substantive and robust data protection regime established by the GDPR of much of its actual protection of data subjects from government surveillance and use of their personal information - although effectiveness with respect to private sector and commercial actors may be more easily upheld and enforced.

4.2 China’s Cybersecurity Law
4.2.1 The data protection regime

China’s new Cybersecurity Law (CCL) came into force on June 1, 2017, during a year which is described by one close observer as “a ground-breaking year for cybersecurity and data privacy” for China. The law combines elements of network governance and security with a regime for personal data protection and adopts and modifies existing laws, measures, and guidelines that address personal data protection in several sector-specific contexts.

A national rather than a regional regulation, the CCL differs from the GDPR in its territorial and jurisdictional scope, furthermore, its approach to the issue of extraterritorial jurisdiction with respect to personal data protection is ambiguous. On the one hand, Article 2 specifically prescribes the CCL’s applicability within national borders, and personal data that is processed by critical information infrastructure operators (a term that remains vague) must remain within the territory of China. On the other hand, Article 5 provides “The State takes measures for monitoring, preventing, and handling network security risks and threats arising both within and without the mainland territory of the People's Republic of China”.  

---

68 See DLA PIPER, supra note 66.  
70 CCL, supra note 14, art. 37 (stating, “Personal information and other important data gathered or produced by critical information infrastructure operators during operations within the mainland territory of the People's Republic of China, shall store it within mainland China,” although exceptions are permitted); CCL, supra note 14, art. 2 (stating “This law applies with respect to the construction, operation, maintenance and usage of networks, as well as network security supervision and management within the mainland territory of the People's Republic of China.”) (emphasis added)).  
71 CCL, supra note 14, art. 5 (emphasis added).
Regarding the substantive balance between individual data privacy rights and national security considerations, the CCL draws on the approach of the March 2017 International Strategy on Cooperation for Cyberspace, which stipulates that:

China…fully respects citizens' rights and fundamental freedoms in cyberspace and safeguards their rights to be informed, to participate, to express and to supervise while protecting individual privacy in cyberspace. [....]. China pursues effective governance in cyberspace to promote free flow of information while ensuring national security and public interests. 72

Yet, as in other domestic jurisdictions, these latter national security and public interest considerations are often, if not always, prioritized by government regulators. The Chinese approach to prioritization of national sovereignty over individual freedoms in cyberspace, called “cyber sovereignty”, confirms this hierarchy and points to a calibration of data protection and national security considerations that reflect a particular policy agenda. 73 In the words of one close observer:

The core assertions in this [cyber sovereignty] agenda are that national boundaries should exist in the virtual environment just as they do in the real world, and that governments should be the dominant norm setters. This runs counter to the multi-stakeholder, open model for internet governance defended by the US, and espoused by many in the global internet governance community. 74

Specifically, while the CCL shares with the EU the goal of providing a comprehensive approach to personal data protection, 75 its basic approach of prioritizing national security and defense considerations to promote cyber sovereignty is fundamentally different from the

---


74 Rogier Creemers, The Chinese Cyber-Sovereignty Agenda, in CONNECTIVITY WARS: WHY MIGRATION, FINANCE AND TRADE ARE THE GEO-ECONOMIC BATTLEGROUNDS OF THE FUTURE 120, 122 (M. Leonard ed., 2016). Creemers adds his appraisal of some of the motivations for the cyber sovereignty approach: “China’s chief concern is domestic: that the internet might be used as a conduit for political destabilisation and economic immobilsation . . . Moreover, the Snowden revelations have encouraged the idea that acquiring information through espionage is crucial to China’s security.” Id. at 124-125.

The abovementioned “open model of internet governance” held by many Western democracies.\textsuperscript{76} Thus, the CCL incorporates provisions requiring electronic identity verification of data subjects,\textsuperscript{77} censorship of user content,\textsuperscript{78} and close cooperation with government authorities by network operators.\textsuperscript{79} Further rule of law aspects will be explored in section 4.2.2 below.

Article 1 of the CCL addresses the national security-privacy dilemma by setting out both of these principles – national security and citizens’ rights – as underlying purposes of the law:

This Law is developed \textbf{for the purposes of guaranteeing cybersecurity, safeguarding cyberspace sovereignty, national security and public interest,} protecting the \textbf{lawful rights and interests of citizens,} legal persons and other organizations, and promoting the \textbf{sound development of economic and social informatization}.\textsuperscript{80}

It is significant to note that, while “lawful rights and interests of citizens” are mentioned, the specific right to data protection in cyberspace is not. This absence contrasts with the GDPR’s Article 1, which provides that the regulation “protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data”.\textsuperscript{81}

In many respects, the regulatory modalities of the CCL to protect personal data appear to be comparable to those of the GDPR.\textsuperscript{82} First, the definition of protected personal data in Article 76(5) is similar to that in GDPR Article 4(1), \textit{i.e.}, any information that can be used to determine the identity of a natural person, either independently or by cross-reference.\textsuperscript{83} Second, collection and use of personal data by “network operators” – network owners, network administrators, and network service providers\textsuperscript{84} – requires data subject consent;\textsuperscript{85} and Chapter IV of the CCL, entitled “Network Information Security”, stipulates several rights of Chinese data subjects, including the preservation of confidentiality, and the right to correct

\textsuperscript{76} Greg Austin, \textit{International Legal Norms in Cyberspace: Evolution of China’s National Security Motivations, in INTERNATIONAL CYBER NORMS: LEGAL, POLICY AND INDUSTRY PERSPECTIVES} 171 (Anna-Maria Osula & Henry Roigas eds., 2016); DLA PIPER, \textit{supra note 66}.
\textsuperscript{77} CCL, \textit{supra note 14, art. 24}.
\textsuperscript{78} Id. arts. 47 and 48.
\textsuperscript{79} Id. art. 28.
\textsuperscript{80} Id. arts. 5, 8, 12 (addressing national security and law enforcement authorities of the government) (emphasis added).
\textsuperscript{81} GDPR, \textit{supra note 13, art. 1}. These rights are referenced, as well, in Article 2 of the EU’s 2016 Network Security Directive, \textit{supra note 67, art. 2}.
\textsuperscript{83} Compare CCL, \textit{supra note 14, art. 76.5, with GDPR, supra note 13, art. 4}.
\textsuperscript{84} CCL, \textit{supra note 14, art. 76}. Networks are systems consisting of computers or other data terminal equipment and relevant devices that collect, store, transmit, exchange, and process information.
\textsuperscript{85} Id. arts. 22, 41.
Third, in the event of a data breach that compromises confidentiality or is likely to do so, network operators are required to mitigate damages and inform both data subjects and government regulators. The CCL also establishes significant sanctions for abuse of protected personal data; the illegal accessing, sale, or provision of such data may be punished by a fine up to ten times the illegally-obtained income or criminal detention. In September 2017, ten leading online service providers signed a governmental memorandum committing to best practices for personal data protection as part of the implementation of the CCL.

In addition to these CCL provisions, criticized by many observers for their non-specificity and the practical difficulties the present for organizations, China’s Standards Administration has published a national standard on personal information protection entering into force in May 2018. Titled GB/T 35273-2017 Information Technology – Personal Information Security Specification, this non-binding standard represents best practice guidance for organizations operating in China with respect to data protection modalities, such as elements that should be included in privacy notices, instructions for obtaining consent from minors, and specific documentation requirements for data transfers.

### 4.2.2 Rule of law constraints

The CCL includes in its Article 41 the rule of law basis for data collection and processing on the part of commercial organizations, including constraints on the legality of processing, as follows:

Network operators collecting and using personal information shall abide by the principles of legality, propriety and necessity; make public rules for collection and use, explicitly stating the purposes, means, and scope for collecting or using information, and obtaining the consent of the person whose data is gathered.

Network operators must not gather personal information unrelated to the services they provide; must not violate the provisions of laws, administrative regulations

---

86 Id. at art. 30.
87 Id. at art. 43. Similar modalities obtain under other Chinese data protection regulations that were promulgated prior to the CCL and are still in force. See DLA Piper, supra note 66, at 4-5.
88 CCL, supra note 14, art. 63.
92 Id.
or agreements between the parties to gather or use personal information; and shall follow the provisions of laws, administrative regulations and agreements with users to process personal information they have stored.93

In contrast, with respect to the activities of governmental bodies with respect to data collection, the CCL is much more reserved. In fact, it avoids carving out national security and law enforcement exceptions. Where the GDPR stipulates criteria for the legality of personal data processing and limits the parameters of security, defense, and other exceptions using constitutional and administrative law,94 the CCL provides broad authority for national agencies charged with ensuring network security “within the scope of their responsibilities” and in accordance with relevant laws and regulations.95 The limitations on these authorities are minimal and currently lack clear legal criteria, as we shall show herein.

Moreover, beyond some of the prima facie similarities with the GDPR in its modalities of data protection, the underlying rule of law assumptions at the basis of the CCL are radically different. In particular, the CCL contains three important parameters that differ significantly from the GDPR regime: (a) substantive limitations on the use of cyber networks by data subjects; (b) data localization requirements; and (c) the relative lack of restrictions on the violation of data privacy rights by network suppliers and national agencies responsible for network security.

First, Article 12 specifies regulatory parameters for the use of cyber networks in China. On the one hand, it establishes the state’s obligation to protect “the rights of citizens” and guarantees the “lawful, orderly and free circulation of network information.” On the other hand, it establishes sweeping limitations on individuals’ cyberspace activities:

Any person and organization using networks shall abide by the Constitution and laws, observe public order and respect social morality; they must not endanger network security, and must not use the network to engage in activities endangering national security, national honor and interests, inciting subversion of national sovereignty, the overturn of the socialist system, inciting separatism, undermining national unity, advocating terrorism or extremism, inciting ethnic hatred and ethnic discrimination, disseminating violent, obscene or sexual information, creating or disseminating false information to disrupt the economic or social order, as well as infringing on the reputation, privacy, intellectual property or other lawful rights and interests of others…96

93 CCL, supra note 14, art. 41.
94 GDPR, supra note 13, art. 23.
95 CCL, supra note 14, art. 8.
96 CCL, supra note 14, art. 12 (emphasis added).
Supporting the implementation of Article 12 and the CCL overall, Article 24 requires network service providers to condition network access for data subjects on the provision of “real identity information” in signed agreements. This requirement applies to all network access and domain registration services.\(^97\) Although service providers are bound to keep this personal data confidential and must abide by the principles of legality, legitimacy and necessity in utilizing it,\(^98\) there are no apparent legal restrictions on either government access or use.\(^99\) No necessity, proportionality, or other constraints are evident. This mandatory abdication of data privacy with respect to government authorities is likely to have a chilling effect on data subjects’ use of cyber networks.\(^100\)

Second, in addition to this broad prescriptive limitation on individual rights of free speech and the free flow of information, a data localization requirement applies to protected personal information and other “important data” gathered and created in China, processed by critical information infrastructure operators, a requirement that is now intended to encompass all network operators.\(^101\) Thus, without showing a “genuine business need” and passing a governmental security assessment, protected personal data and other “important” data must remain on servers physically located within China’s territory.\(^102\)

---

\(^97\) This identification requirement also appears in the Decision on Strengthening Online Information Protection of December 2012, supra note 68, art. 6 (“Network service providers that handle website access services for users, handle fixed telephone, mobile telephone and other surfing formalities, or provide information publication services to users, shall, when concluding agreements with users or affirming the provision of service, require users to provide real identity information.”). Users also need to supply their identities for the use of mobile apps. See Rogier Creemers, Mobile Internet Application Programs , art. 7(1), CHINA COPYRIGHT & MEDIA (June 28, 2016), https://chinacopyrightandmedia.wordpress.com/2016/06/28/mobile-internet-application-information-service-management-regulations/ (unofficial English translation).

\(^98\) CCL, supra note 14, arts. 2-3.

\(^99\) Id. art. 24. In fact, the government implements a “network identity credibility strategy” using identity confirmation technologies and supporting exchange of personal identity information among “different electronic identity confirmations.


Third, in upholding the two previous mandates, national authorities are granted broad powers to carry out network security. Article 8 is the relevant provision, which stipulates:

The State network information departments are responsible for comprehensively planning and coordinating network security efforts and related supervision and management efforts. The State Council Departments for telecommunications, public security, and other relevant organs, are responsible for network security protection, supervision and management efforts within the scope of their responsibilities, in accordance with the provisions of this Law, relevant laws and administrative regulations.103

The use of protected personal data by government agencies, under the authority set out in Article 8, is subject to two criteria in the CCL. First, Article 30 requires that information obtained by government agencies for network security purposes must not be used for other purposes.104 Second, Articles 14 and 45 require that such data remain “strictly confidential,” and not be leaked, sold, or unlawfully provided to others, although the criteria for protection are not specified.105 If additional constraints exist on organizational mandates to process personal data of these national authorities, they are extraneous to the CCL and not transparently reflected in its text.106

Ostensibly, these provisions provide a strong bias in cyberspace activity on the part of data subjects in China favoring national security – what might be called “public order” in its broadest sense in Western democracies – over the protection of their personal data. There may be additional limitations on the legality of supervisory and surveillance activities by state security organs in the laws governing the activities of these bodies, yet they are not explicit in the data protection regime itself. This point needs further clarification and study. Full enforcement of the CCL in coming years is liable to severely reduce the free flow of information in general and produce a chilling effect on individual use of the internet and other cyber-enabled means of communication due to the hobbling of individual data protection. This aim is consistent with China’s overall approach to network security and cyber sovereignty.107

---

103 CCL, supra note 14, art. 8.
104 Id. art. 30.
105 Id. art. 14 (“Relevant departments shall preserve the confidentiality of the informants’ information and protect the lawful rights and interests of the informants’); id. art 45.
106 There are several references to the requirement of network operators and government bodies to act in conformity with laws and regulations and, in CCL Article 12, the Constitution, which protects data subject rights in its Article 40; but the parameters of these constraints remains unclear.
5. Comparisons and conclusions: towards a better understanding of “cyber privacy”

In this article, we aimed to show that the regulatory models for personal data protection put forward in the EU’s GDPR and China’s CCL provide insights into how a more general understanding may be gleaned of the protection of personal data as an integral part of national and regional cybersecurity norms.

The regulatory efforts of these two major jurisdictions embody models that exhibit an interesting combination of converging modalities and diverging regulatory approaches. On the one hand, the definitions of personal data and many of the modalities for personal data protection are remarkably similar in the GDPR and the CCL. On the other hand, rule of law considerations, including the scope of legal constraints on government agencies in exercising their authority to protect national security through regulatory carve-outs, differ fundamentally. While the GDPR incorporates within its “exemptions regime” an explicit set of constraints on permissible curtailment by government of the fundamental right of individual data privacy, the CCL lacks specific and transparent provisions regarding legal constraints on government collection, use and retention of personal data.

This is a significant distinction in terms of the rule of law, at least in terms of the Western democratic version of this concept which aims to include transparent constraints on government activities. In this vein, the 2011 Report of the UN Special Rapporteur noted that:

[T]he right to privacy can be subject to restrictions or limitations under certain exceptional circumstances. This may include State surveillance measures for the purposes of administration of criminal justice, prevention of crime, or combating terrorism. However, such interference is permissible only if the criteria for permissible limitations under international human rights law are met. Hence, there must be a law that clearly outlines the conditions whereby individuals’ right to privacy can be restricted under exceptional circumstances.108

In line with the Special Rapporteur’s view, criteria for swaying the balance away from individual privacy rights and towards national security considerations should be transparent within the statutory regime, so that judicial review of national security and other exceptions is feasible, practicable and readily available to data subjects who want to

contest carve-outs. Both the GDPR and the CCL fall short of the ideal to different degrees.

Nonetheless, the engagement of these two significant jurisdictions with the challenge of protecting personal data protection in balance with security considerations in cyberspace – cyber privacy – highlights its criticality. As discussed above, data protection is emerging as an essential element of international cybersecurity and stability. The time is ripe for a normative merger that will narrow the conceptual gaps with respect to cybersecurity at the national level, and significantly re-distribute cyber risks that stem from the vulnerability of personal data through the explicit imposition of regulatory responsibility and accountability upon corporations and individuals.

We have yet to fully engage with this challenge at the multi-lateral, international level and in many domestic jurisdictions. The EU and China regulatory models draw global attention to the need for more robust and transparent balancing mechanisms between cybersecurity needs and privacy rights, ultimately contributing towards increased levels of cyber stability and security overall. The difficult challenge that lies ahead is the coordination at the regional and global levels of emerging cyber privacy regimes such as the GDPR and the CCL, in order to better leverage the regulatory tools that are becoming increasingly available for achieving this common aim.

***