Annotated Bibliography on Chinese Surveillance and European Union Data Privacy

Peter Swire[1]

This document collects sources relevant to the topic of Chinese surveillance practices and European Union data protection requirements. The aim of this document is to provide references, briefly summarized, to informative and publicly available documents.

In July, 2019 the Court of Justice for the European Union hears arguments in "Schrems 2," to consider whether there are adequate protections when personal data is transferred to the United States under standard contract clauses. The central issue in the case is whether the legal safeguards in the U.S. are sufficient concerning government surveillance. If the CJEU holds in favor of Schrems, then there may be major restrictions on the lawfulness of transferring personal data from the EU to the U.S. Such restrictions would block many commercial arrangements between the EU and the U.S.

This document is being published in tandem with Peter Swire's opinion piece in Le Monde, entitled "Les Etats-Unis, la Chine et les potentielles nouvelles restrictions au transfert global de données personnelles." ("The United States, China, and potential new restrictions on the global transfer of personal data."). That article discusses what would happen if Schrems were to win, as he did in striking down the EU/U.S. Safe Harbor in 2015. The focus of the Le Monde article is an issue that will then arise – would such restrictions apply only to transfers to the United States? Or would they also apply to nations, such as China, that have far weaker protections against excessive government surveillance?

This annotated bibliography documents the following results of our research:

1. Surveillance within China is extensive.
2. Substantial and growing amounts of personal data are flowing from other countries, such as EU Member States, to China and Chinese companies.
3. China lacks rule-of-law safeguards against excessive surveillance, and personal data held by companies in China is accessible to the government.
4. By contrast, the United States has long-standing and extensive safeguards against excessive government surveillance.
5. As discussed in Le Monde, allowing data transfers to China while blocking them to the U.S. would be legally unjust and would cause large and negative consequences.

[1] Peter Swire is the Elizabeth & Tommy Holder Chair of Law and Ethics at the Georgia Tech Scheller College of Business. He is also Research Director of the Cross-Border Data Forum, Senior Fellow with the Future of Privacy Forum, and Senior Counsel with Alston & Bird LLC. This research was funded by an Andrew Carnegie Fellowship, the Future of Privacy Forum, and the Georgia Tech Cross-Border Access to Data Project. For assistance in the research, special thanks to DeBrae Kennedy-Mayo and Amy Oliver for substantial research, and as well to Justin Hemmings and Sreenidhi Srinivasan for their assistance.

1. Surveillance Within China Is Extensive.

Part 1 addresses major categories of surveillance within China: (a) the social credit system; (b) video surveillance and facial recognition; (c) DNA and biometrics; (d) voiceprint database; (e) predictive policing; (f) artificial intelligence; (g) digital identity; (h) "Great Firewall of China"; (i) virtual private networks (VPNs); (j) encryption; (k) real-name identification; (l) technology transfers and access to business information; (m) cloud services and localization.

a. Social Credit System

Big Data and the Social Credit System: The Security Consequences
Report: Rethinking Security: China and the Age of Strategic Rivalry – Highlights from an Academic Outreach Workshop
Canadian Security Intelligence Service (2018)
https://www.canada.ca/en/security-intelligence-service/corporate/publications/china-and-the-age-of-strategic-rivalry/big-data-and-the-social-credit-system-the-security-consequences.html
"As the social credit system develops and as participation extends, firms participating in joint ventures with Chinese companies, companies doing business in the PCR or individuals living in or working with Chinese entities, may be required or compelled to participate in the system."

China has started ranking citizens with a creepy 'social credit' system — here's what you can do wrong, and the embarrassing, demeaning ways they can punish you
By Alexandra Ma
Business Insider (Oct. 29, 2018)
https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4
"The Chinese state is setting up a vast ranking system that will monitor the behavior of its enormous population and rank them all based on their 'social credit.'"

"The 'social credit system,' first announced in 2014, aims to reinforce the idea of 'keeping trust is glorious and breaking trust is disgraceful,' according to a government document."

A low Social Credit Score (SCS) may result in travel restrictions, slow internet speeds, reputational sanctions on public websites, diminishment of employment prospects in the civil service, and even having a pet taken away. Children of those with low ratings may also be prohibited from attending private schools.

China's Social Credit System: A Mark of Progress or a Threat to Privacy?
By Martin Chorzempa, Paul Triolo, and Samm Sacks
Peterson Institute for International Economics (June 2018)
https://www.piie.com/publications/policy-briefs/chinas-social-credit-system-mark-progress-or-threat-privacy
"The fundamental premise of the 2014 [Social Credit Score] plan is that current governance tools and methods are insufficient to solve China's greatest challenges … The plan document cites a laundry list of social ills that stem from the lack of trust and trustworthiness at all levels of a

fragmented Chinese society. These include tax evasion, factory accidents, food and drug safety scares, fraud, academic dishonesty, and rampant counterfeiting of goods."

"The SCS has two main components. The first is what may become the world's largest dataset, integrating currently disconnected data held by government and nongovernmental entities across China and expanding data collection efforts. The plan calls for "interconnection and interactivity of…credit information systems and…networks that cover all information subjects, all credit information categories, and all regions nationwide" (State Council 2014).

"If China's social credit plan is successful, other authoritarian regimes could be inspired to emulate its model."

China's social credit system 'could interfere in other nations' sovereignty
By Kelsey Munro
The Guardian (Jun. 27, 2018)
https://www.theguardian.com/world/2018/jun/28/chinas-social-credit-system-could-interfere-in-other-nations-sovereignty
As of January 1, 2018, all companies with a Chinese business license – which is required of every company operating in the country – came into the social credit system through the new license requirement to have a "unified social credit code."

In a new report, US China scholar Samantha Hoffman of the ASPI International Cyber Policy Institute in Canberra discussed recent incidents where international airlines in both the US and Australia were pressured by Chinese authorities to adopt Beijing's preferred terminology to refer to Taiwan and Hong Kong. According to the report, "Social credit was used specifically in these cases to compel international airlines to acknowledge and adopt the CCP's" terminology.

In an interview with the Guardian Australia, Hoffman said, "Companies don't have a choice but to comply if they want to continue doing business in China."

China's Surveillance State Should Scare Everyone
By Anna Mitchell & Larry Diamond
The Atlantic (Feb. 2, 2018)
https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203
Currently voluntary as a private sector enterprise effort to rate creditworthiness, the SCS will become a mandatory government program by 2020. "China's evolving algorithmic surveillance system will rely on the security organs of the Communist party-state to filter, collect, and analyze staggering volumes of data flowing across the internet."

The Transparent Self under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System
By Yongxi Chen and Anne S.Y. Cheung
University of Hong Kong Faculty of Law Research Paper (June 27, 2017)
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2992537
Scholars from the University of Hong Kong refer to the SCS as "essentially an all-encompassing, penetrative system of personal data processing, manifested by the comprehensive collection and

expansive use of personal data with the explicit intention on the Chinese government's part of harnessing the ambition and power of big data technology."

China: When Big Data Meets Big Brother
By Charles Clover
Financial Times (Jan. 19, 2016)
https://www.ft.com/content/b5b13a5e-b847-11e5-b151-8e15c9a029fb
Anne Stevenson-Yang, the head of a Beijing-based consulting firm, has said that the SCS is being developed to foster "greater social control and public morality." Stevenson-Yang has compared the SCS to the personal surveillance common under former Chinese leader Mao Zedong, when personal files were maintained by work units and "busybodies in every neighbourhood kept authorities informed of the minutiae of daily life."

China employs two million microblog monitors state media say
BBC News (Oct. 4, 2013)
https://www.bbc.com/news/world-asia-china-24396957
In 2013 Beijing News reported that more than two million people monitor web activity or microblogs for the government. The monitors or "internet opinion analysts" are employed by the state and commercial entities. Reports suggest that websites outside of China are also monitored.

b. Video Surveillance and Facial Recognition

China's watchful eye: Beijing bets on facial recognition in a drive for total surveillance
By Simon Denyer
The Washington Post A1 (Jan. 7, 2018)
https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/?utm_term=.81d26969beb0
The Chinese government seeks to develop a video surveillance network by 2020 that is "omnipresent, fully networked, always working and fully controllable" according to official documents. News reports claim that China is building the world's largest and most sophisticated video surveillance system.

Facial recognition and other technologies are being deployed with video surveillance to create nationwide surveillance and data sharing system. Data generated by new technologies permit Chinese police and security authorities to implement "Xue Liang," which is translated as "Sharp Eyes." Authorities are linking public and private video systems throughout the country with other collected data to increase the scope of the surveillance and data sharing. "The goal, according to tech industry executives working on it, is to shine a light on every dark corner of China, to eliminate the shadows where crime thrives." Security cameras from shopping malls and private buildings to transportation centers are being integrated into a nationwide, data-sharing system.

Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life
By Josh Chin and Clément Bürge
The Wall Street Journal (Dec. 19, 2017)

https://www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355
Another use of data that is collected is to combine video surveillance with license plate readers to permit authorities to identify out-of-town license plates; this then allows law enforcement to question the occupants because they are not local residents.

In Your Face: China's all-seeing state
By John Sudworth
BBC News (Dec. 10, 2017)
http://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state
In December 2017, the BBC reported that Chinese authorities could identify its correspondent in a metropolitan area of about four million residents in approximately seven minutes using video and facial recognition technology.

China to have 626 million surveillance cameras within 3 years
By Frank Hersey
technode (Nov. 22, 2017)
https://technode.com/2017/11/22/china-to-have-626-million-surveillance-cameras-within-3-years/
The number of security cameras in China is estimated to grow from 176 million in 2017 to possibly 626 million by 2020.

c. DNA and Biometrics

China Snares Innocent and Guilty Alike to Build World's Biggest DNA Database
By Wenxin Fan, Natasha Khan, and Liza Lin
The Wall Street Journal (Dec. 26, 2017)
https://www.wsj.com/articles/china-snares-innocent-and-guilty-alike-to-build-worlds-biggest-dna-database-1514310353

DNA and biometrics data collection (beyond facial recognition) feature prominently in China's data collection strategy. *The Wall Street Journal* reports that efforts are underway in China to nearly double the size of the "world's biggest DNA database" from 54 million to 100 million records by 2020. DNA collection through saliva swabs and blood samples is common in China for minor infractions such as forgetting an identification card, as well for writing blogs critical of the government and for being a member of group that is considered to be a risk to social stability. It has been asserted that "Across China, anyone stopped in the street by police can wind up in the database."

Some of the most detailed information about DNA and biometric data collection in China comes in the northwestern region of Xinjiang. In six defined geographic areas within Xinjiang, police officers must collect pictures, fingerprints, blood type, DNA, and iris scans as part of this collection effort. This is the first region in China to extensively collect such data. The regional policy also requires DNA collection from all residents of Xinjiang when they renew or replace identification cards.

Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life
By Josh Chin and Clément Bürge
The Wall Street Journal (Dec. 19, 2017)
https://www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355
The Wall Street Journal reported a specific example of this biometric data collection effort involving a Uighur poet and filmmaker. According to the poet, he, his wife, and other Uighurs were called to a local police station in May 2017 and told to provide samples. He provided blood samples and fingerprints and was then required to read a newspaper for two minutes to record his voice.

d. Voiceprint Database

China: Voice Biometric Collection Threatens Privacy
By Human Rights Watch (Oct. 22, 2017)
https://www.hrw.org/news/2017/10/22/china-voice-biometric-collection-threatens-privacy
China is reportedly collecting voiceprints to develop a database for the identification of voices in phone conversations.

China's A.I. Advances Help Its Tech Industry, and State Security
By Paul Mozur & Keith Bradsher
The New York Times (Dec. 3, 2017)
https://www.nytimes.com/2017/12/03/business/china-artificial-intelligence.html
To develop the system, authorities are working with iFlytek - a Chinese company that produces the majority of speech recognition technology in China. The *New York Times* reported in 2017 that iFlytek's maintains ties with the government and is viewed as an "ally of the government." The *Time*s also reported that a government security official stated voiceprint identification is equivalent to video or fingerprint information.

Company in Focus: China's leader in voice recognition AI goes global
By Shunsuke Tabeta
Nikkei Asian Review (Feb. 1, 2018)
https://asia.nikkei.com/magazine/20180201/Business/Company-in-focus-China-s-leader-in-voice-recognition-AI-goes-global?page=2
China Mobile, a state-owned communications company, is the biggest shareholder of iFlytek.

e. Predictive Policing

China's Algorithm of Repression
Reverse Engineering a Xinjiang Police Mass Surveillance App
Human Rights Watch (May 1, 2019)
https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance

"[T]he IJOP app fulfill[s] three broad functions: collecting personal information, reporting on activities or circumstances deemed suspicious, and prompting investigations of people the system flags as problematic … Analysis of the IJOP app reveals that authorities are collecting massive amounts of personal information—from the color of a person's car to their height down to the precise centimeter—and feeding it into the IJOP central system, linking that data to the person's national identification card number. Our analysis also shows that Xinjiang authorities consider many forms of lawful, everyday, non-violent behavior—such as 'not socializing with neighbors, often avoiding using the front door'—as suspicious. The app also labels the use of 51 network tools as suspicious, including many Virtual Private Networks (VPNs) and encrypted communication tools, such as WhatsApp and Viber."

About to Break the Law? Chinese Police Are Already On To You: Rights group says 'predictive policing' platform combines feeds from surveillance cameras with personal information
By Josh Chin
The Wall Street Journal (Feb. 27, 2018)
https://www.wsj.com/articles/china-said-to-deploy-big-data-for-predictive-policing-in-xinjiang-1519719096
Law enforcement authorities in China have benefitted from access to aggregated data and new technologies. Officials in Xinjiang have implemented a "Integrated Joint Operations Platform" (Platform) that reportedly combines personal information through video, phone, travel, and religious organization records to identify persons they consider suspicious, turning the region "into a laboratory for cutting-edge surveillance and social control."

Authorities have also installed high-definition cameras with facial recognition capabilities and hand-held smartphone scanners. Local officials generate lists from the integrated data that are used by police for investigative purpose. Installation of the Platform in local governments began in 2016. The China Electronics Technology Group or CETC, a state-owned company, provides the technology used to implement the Platform. Human rights advocates note that the policing is largely aimed at the Uighur.

How Does Face-Recognition Sunglasses Work?: Chinese Police Increase Use of Smart Tech
By Shreesha Ghosh
International Business Times (Feb. 9, 2018)
http://www.ibtimes.com/how-does-face-recognition-sunglasses-work-chinese-police-increase-use-smart-tech-2651700
According to government officials, the use of the glasses at the Zhengzhou East Railway Station in Henan province resulted in the identification of 26 people trying to use other people's identification and seven fugitives being taken into custody. The smart glasses work by comparing a picture taken through the technology to information in a database or "blacklist" maintained in a connected mobile device with the officer. LLVision Technology Co., a domestic company, developed the glasses used in Zhengzhou.

Police in China Start Wearing Facial-Recognition Glasses
By Matthew Humphries
PCMag (Feb. 8, 2018)

https://www.pcmag.com/news/359096/police-in-china-start-wearing-facial-recognition-glasses
In addition to access to real-time video feeds that can identify individuals, police are being issued smart glasses that not only identify people on the street through facial recognition technology, but also link the face and name to other data.

f. Artificial Intelligence

.

U.S. and Chinese Companies Race to Dominate AI: Chinese rivals are gaining fast because of rising investment, as well as freer access to enormous amounts of data about people
By Sam Schechner, Douglas MacMillan, and Liza Lin
The Wall Street Journal (Jan. 18, 2018)
https://www.wsj.com/articles/why-u-s-companies-may-lose-the-ai-race-1516280677
China's strategic plans state that it seeks to be the world's leader in AI by 2030 and has committed significant funding to the effort.

In developing AI, there are close links between the private and government sectors: Chinese companies in many instances have access to vast amounts of data that is "often compiled with the help of government agencies."

g. Digital Identity

China Plans To Turn Country's Most Popular App, WeChat, Into An Official ID System
By Glyn Moody
TechDirt (Jan. 4, 2018)
https://www.techdirt.com/articles/20180103/04003638918/china-plans-to-turn-countrys-most-popular-app-wechat-into-official-id-system.shtml
According to the South China Morning Post, "The government of Guangzhou, capital of the southern coastal province of Guangdong, started on Monday a pilot programme that creates a virtual ID card, which serves the same purpose as the traditional state-issued ID cards, through the WeChat accounts."

This is "an extremely powerful way for the Chinese government to implement its real-name policy for online activities, something that it has so far failed to push through. It will mean that the daily posts and transactions carried out using a mobile will not only be available to the Chinese authorities but will be unambiguously linked to an individual."

The Internet Tightens: Popular Chinese WeChat App to Become Official ID
By Alyssa Abkowitz
The Wall Street Journal (Dec. 31, 2017)
https://www.wsj.com/articles/internet-tightens-popular-chinese-wechat-app-to-become-official-id-1514541980
WeChat, a "super app" that started out as a messaging service, is now part of pilot program to create a digital identity card that will replace the state-issued cards needed to access services.

Big Brother collecting big data – and in China, it's all for sale
By Saša Petricic
CBC News (Jan. 11, 2017)
http://www.cbc.ca/news/world/china-data-for-sale-privacy-1.3927137
The government restrictions on WeChat follow Chinese students studying abroad.

h. Great Firewall of China

The Great Firewall of China: Xi Jinping's Internet Shutdown
By Elizabet Economy
The Guardian (June 29, 2018)
https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown
"By 1997, Beijing had enacted its first laws criminalising online postings that it believed were designed to hurt national security or the interests of the state."

"In 1998, a 30-year-old software engineer called Lin Hai forwarded 30,000 Chinese email addresses to a US-based pro-democracy magazine. Lin was arrested, tried and ultimately sent to prison in the country's first known trial for a political violation committed completely online."

"The following year, the spiritual organisation Falun Gong used email and mobile phones to organise a silent demonstration of more than 10,000 followers around the Communist party's central compound, Zhongnanhai, to protest their inability to practise freely. The gathering, which had been arranged without the knowledge of the government, precipitated an ongoing persecution of Falun Gong practitioners and a new determination to exercise control over the internet."

China Protectionism Creates Tech Billionaires Who Protect Xi
By Shelly Banjo
Bloomberg Technology (March 6, 2018)
https://www.bloomberg.com/news/articles/2018-03-06/how-china-protectionism-creates-tech-billionaires-who-protect-xi
News reports indicate that the "Great Firewall has also been a boon for homegrown internet focused businesses. The system of control and outright blockades effectively keeps Facebook, Twitter, Snapchat, YouTube, Google and others locked out of the world's biggest tech playground."

The Evolution of China's Great Firewall: 21 Years of Censorship
By Jimmy Wu and Oiwan Lam
Hong Kong Free Press (September 3, 2017)
https://www.hongkongfp.com/2017/09/03/evolution-chinas-great-firewall-21-years-censorship/
"In 1996, Beijing enacted a set of interim provisions for governing computer information, and in 1998, the Ministry of Public Security launched the Golden Shield project — a national filter that blocks politically sensitive content from entering the domestic network. This censorship tactic

scheme has long been nicknamed the Great Firewall, and has undergone periodic upgrades since it was first introduced."

Below is a summary of the stages:
- "First stage: The Golden Shield blocks domain names and IP addresses"
- "Second stage: The Golden Shield implements keyword censorship"
- "Third Stage: Great Firewall begins detecting VPNs and other circumvention tools"
- "Fourth Stage: Cyber security laws target anonymity and VPNs"

"On June 1 [2017], the controversial "Cyber Security Law" officially took effect, giving far-reaching rights to the supervision department, strengthening internet operator responsibilities and duties, and demanding real-name registration of individual internet users …The legislation directly compelled Apple to take down VPN apps from its China app store in July. Amazon's China partner also issued a warning to its customers against the use of its cloud server for setting up a VPN server."

China's technology protectionism and its non-negotiable rationales
By Martina F. Ferracane and Hosuk Lee-Makiyama
European Centre for International Political Economy (June 2017)
http://ecipe.org/publications/chinas-technology-protectionism/?chapter=all
The golden shield "system is based on centralised control over international gateways, filtering online content or blocking access entirely to some of the most common websites on the public internet, and the authorities have also shut down online access to entire communications systems in response to specific events, notably imposing a 10-month internet blackout in the Xinjiang Uighur Autonomous Region in 2009 to quell 'social unrest.'"

The Great Firewall of China: A Technical Perspective
Torfox: A Stanford Project (May 30, 2011)
https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/great-firewall-technical-perspective/index.html
"The Great Firewall uses three distinct types of methods to block access to websites in China. They are as follows: 1. IP blocking; 2. IP address misdirection; and 3. data filtering."

China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China
By Greg Walton
International Center for Human Rights and Democratic Development (2001)
https://books.google.com/books?id=S9rP0A2q14UC&printsec=frontcover#v=onepage&q&f=false
"China's Golden Shield project threatens the protection of human rights, in particular the right to privacy - a right that underpins other essential elements of other essential elements of democracy activism such as freedom of association and freedom of expression. It positions the alliance of government and business in opposition to those standing on the cyber-frontline of the human rights movement in China today."

i. VPNs

China's VPN Crackdown May Aid Government Surveillance: It threatens to make emails and data transmissions by foreign companies more vulnerable, security analysts say
By Liza Lin & Yoko Kubota
The Wall Street Journal (Jan. 17, 2018)
https://www.wsj.com/articles/chinas-vpn-crackdown-may-aid-government-surveillance-1516189155
Virtual private networks or VPNs permit users to securely access and send information and have been used by individuals in China to access blocked content - thereby bypassing the controls of the Great Firewall. In 2017, China's Ministry of Industry and Information Technology issued a notice stating that access to non-licensed VPNs will be blocked.

Due to the limited number of licensed VPN providers in the country, state-owned telecommunications companies may benefit from easier access to communications as licensed VPN providers. Further, in 2017, Apple removed nearly 700 VPN apps from its online app store available to Chinese customers in response to government restrictions.

German ambassador Michael Clauss on relations with China, the challenges and potential
By Wendy Wu
South China Morning Post (Dec. 22, 2017)
http://www.scmp.com/news/china/diplomacy-defence/article/2125328/german-ambassador-michael-clauss-relations-china
In a 2017 interview, Germany's ambassador to China, Michael Clauss, echoed Wuttke, by noting, "Secure and undisturbed end-to-end communication is essential for foreign companies and a prerequisite for advanced manufacturing. What especially gives rise to concerns are the uncertainties caused by the opacity of procedures of regulation and standard setting, and the lack of communication with those concerned."

Internet Restrictions Increasingly Harmful to Business, Say European Companies in China
European Union Chamber of Commerce in China news release (Feb. 2, 2015)
http://www.europeanchamber.com.cn/en/press-releases/2235/internet_restrictions_increasingly_harmful_to_business_say_european_companies_in_china
The impact of these government policies is potentially substantial for multinational corporations operating in China. A 2015 survey conducted on behalf of the European Union Chamber of Commerce in China revealed that China's tightening restrictions on domestic internet access may prove "highly detrimental" to European businesses operating in China. Specifically, 86% of respondents noted a negative effect through the blocking of websites and online tools and 80% noted a worsening business impact resulting from the controls. European Chamber President Jörg Wuttke further commented that the internet controls "choke business growth and stifle investment in technology and R&D."

j. Encryption

China's Anti-Terrorism Law Raises Data Security Concerns
By Paul McKenzie et al.
Lawblog (Jan. 20, 2016)
https://www.lexology.com/library/detail.aspx?g=705429e6-d560-4ef9-a415-d34650f3629c
Article 18 of the counter-terrorism law eventually included more general language that telecommunications and internet service providers should "provide technical support and assistance, such as technical interface and decryption, to support the activities of the public security and state security authorities in preventing and investigating terrorist activities."

Encryption and Globalization
By Peter Swire and Kenesa Ahmad
Columbia Science & Technology Law Review (2012)
http://stlr.org/volumes/volume-xiii-2011-2012/encryption-and-globalization/
China considers encryption technology to be subject to government direction and authority rather than a means to encourage private sector development. China's support of indigenous innovation results in strict licensing requirements and attempts to mandate the use of homegrown encryption algorithms that lack any public peer review.

k. Real-Name Identification

China doubles down on real-name registration laws, forbidding anonymous online posts
By Catherine Shu
Techcrunch (Aug. 28, 2017)
https://techcrunch.com/2017/08/27/china-doubles-down-on-real-name-registration-laws-forbidding-anonymous-online-posts/
Network service providers obtain and maintain the data, or "personal electronic information," of users as provided in the 2012 law. The providers must also report illegal content to authorities, with the Cyberspace Administration of China or CAC enforcing the rules.

Real-Name Registration Rules and the Fading Digital Anonymity in China
By Jyh-An Lee & Ching-Yi Lu
Wash. Intl. Law Jour. (Jan. 2016)
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2719384
Real-name registration systems require that users of online services provide personal information to network service providers when signing up for a service so their identity can be verified. National government entities in China considered real-name registration requirements as early as 2003 but did not pass a law until 2012. With the passage of the "Decision of the Standing Committee of the National People's Congress on Strengthening Online Information" on December 28, 2012, China introduced a real-name registration requirement for users of internet services and liability for network service providers who fail to verify that the given name of the user is accurate. Since the name of commentators is known, a real-name registration system forecloses the possibility of anonymous online commentary.

China's Anti-Terrorism Law Raises Data Security Concerns

By Paul McKenzie et al.
Lawblog (Jan. 20, 2016)
https://www.lexology.com/library/detail.aspx?g=705429e6-d560-4ef9-a415-d34650f3629c
Article 21 of the counter-terrorism law requires that operators of certain businesses such as lodging and transportation verify the identities of customers and deny services to customers for whom their identity is unclear or if the customer refuses to participate in the verification process.

l. Technology Transfers and Access to Business Information

Explained, the Role of China's State-Owned Companies
By Amir Guluzade
World Economic Forum (May 7, 2019)
https://www.weforum.org/agenda/2019/05/why-chinas-state-owned-companies-still-have-a-key-role-to-play/
China's efforts to make state-owned enterprises (SOEs) "competitive while holding absolute control over their final decision-making reasserts the Chinese government's commitment to consolidating state control while simultaneously allowing the market to be the ultimate resource allocator."

"[T]he Chinese government is still keen on supporting SOEs and is committed to making them bigger, stronger and more efficient. This is particularly relevant to certain strategic sectors where government oversight is essential - specifically in defense, energy, telecom, aviation and railway systems."

Europe Eyes Privacy Clampdown on China
A Global Standoff over Huawei and Chinese Surveillance is Prompting Europe to Question Whether its Data is Safe in China
By Laurens Cerulus
Politico (February 12, 2019)
https://www.politico.eu/article/european-union-eyes-privacy-clampdown-on-china-surveillance-huawei/
"If the EU starts demanding stricter privacy guarantees from Beijing, Chinese tech giants like e-retailer Alibaba would be the first to feel the heat. Alibaba and companies like Tencent and Huawei already do big business in the EU. Any clampdown on how they access and transfer EU consumers' data could hurt their development in the bloc – and that of the many smaller Chinese players looking to scale up in Europe."

German ambassador Michael Clauss on relations with China, the challenges and potential
By Wendy Wu
South China Morning Post (Dec. 22, 2017)
http://www.scmp.com/news/china/diplomacy-defence/article/2125328/german-ambassador-michael-clauss-relations-china
In 2017, the German ambassador to China stated, "'[m]ore and more German companies approach the embassy and express their grievances about increasing discrimination and obstruction as a result of state intervention and administrative measures. Notorious complaints

about forced technology transfers, compulsory joint ventures in some sectors or the inadequate legal protection of intellectual property have still not been remedied."

US Plans Trade Probe Over China's Demands for Tech Transfers
By Gillian Wong & Jill Colvin
Associated Press (Aug. 2, 2017)
http://www.latimes.com/business/la-fi-china-trade-probe-20170802-story.html
The United States, other governments, and groups representing businesses have accused China of forcing foreign firms to disclose proprietary technology information to gain access to the Chinese market. They argue that the forced technology transfers foster indigenous companies and that the technology is transferred further to those companies, thereby creating great risk for foreign companies and an additional competitive advantage for domestic companies.

Beijing's New National Intelligence Law: From Defense to Offense
By Murray Scot Tanner
Lawfare (July 20, 2017)
https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense
"The new [intelligence] law is the latest in an interrelated package of national security, cyberspace, and law enforcement legislation drafted under Xi Jinping."
"The Chinese Communist Party-state is now strong enough to call for intelligence cooperation even from foreigners doing business in China."

Big Brother collecting big data – and in China, it's all for sale
By Saša Petricic
CBC News (Jan. 11, 2017)
http://www.cbc.ca/news/world/china-data-for-sale-privacy-1.3927137
Government oversight of businesses operating in China is complex and this complexity provides opportunities for data access in the form of regulations, market access restrictions, and promotion of indigenous industry. For example, authorities require private industry to provide control through censorship and surveillance rules that require the companies to "police their own networks."

Systematic government access to private-sector data in China
By Zhizheng Wang
International Data Privacy Law, Vol. 2, No. 4 (2012)
https://academic.oup.com/idpl/article/2/4/220/676863
"Data held in private-sector are compulsorily contributed to the projects and databases in accordance with e-government construction based on the requirements of various laws related to public security, state security, finance, taxation, insurance and so on."

m. Cloud Services and Localization

What China's Cybersecurity Law says about the Future
By Daniel Wagner
International Policy Digest (May 13, 2019)

https://intpolicydigest.org/2019/05/13/what-china-s-cybersecurity-law-says-about-the-future/
To comply with the cybersecurity law's localization requirements, foreign firms are required to invest in new data servers in China, which could be "subject to government spot checks." Requiring entities to establish presence in China could also be a move "to bring data under Chinese jurisdiction to make it easier to prosecute entities seen as violating China's Internet laws."

New cyber security law prompts Amazon to sell part of its China cloud services
By Masha Borak
TechNode (Nov. 11, 2017)
https://technode.com/2017/11/15/new-cyber-security-law-prompts-amazon-to-sell-part-of-its-china-cloud-services/
Provisions of the cybersecurity law result in data localization for Chinese citizen data. Foreign cloud computer providers who operate "critical information infrastructure" must maintain data domestically and offer the service in partnership with a domestic company.

In late 2017, Amazon Web Services or AWS announced the sale of physical infrastructure assets in China to a Chinese company because it cannot operate certain technology under the law.

2. Substantial and growing amounts of personal data are flowing from other countries, such as EU Member States, to China and Chinese companies.

Part 2 addresses the second theme of the research: substantial and growing amounts of personal data are flowing from other countries, such as EU Member States, to China and Chinese companies.

The documents here address: (a) secret collection of data by Chinese entities; (b) Chinese companies in Europe; and (c) Chinese market share in Europe.

a. Secret Collection of Data by Chinese Entities

Beware: China May Be Reading Your Email
By Chris Taylor
Asia Times (Oct. 31, 2018)
https://www.asiatimes.com/2018/10/article/beware-china-may-be-reading-your-email/
"A recent academic report (detailed below) claims that China has been routinely and systematically hijacking internet traffic from the United States, Canada, Europe, and other countries through security flaws in the deep structure of the internet … China Telecom has multiple points of presence (POPs) in North America and Europe and rerouting traffic via ultra-fast fiber-optic cables causes delays to be almost unnoticeable … To put it simply, somebody in Beijing may be receiving and reading your emails before you do, as well as capturing your passwords and other personal data from websites you visit."

China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China's Telecom's BGP Hijacking
By Chris Demchak & Yuval Shavitt
Military Cyber Affairs (2018)
https://scholarcommons.usf.edu/mca/vol3/iss1/7/
According to a report by Chris Demchak, Chair of Cyber Security and Director of the Center for Cyber Conflicts Studies at the U.S. Naval War College, and Yuval Shavitt, Professor of Electrical Engineering and Member of the Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University, China Telecom hijacked domestic US and cross US traffic and redirected it to China over days, weeks, and months as demonstrated in the examples below:
- Canada to Korea in 2016: For approximately 6 months, China Telecom hijacked routes from Canada to Korean government sites.
- U.S. to Italy in 2016: During the month of October, China Telecom hijacked routes from the U.S. to a bank in Milan, Italy.
- Scandinavia to Japan in 2017: During April and May, China Telecom hijacked routes from Sweden and Norway to the Japanese office of a U.S. news agency.
- Italy to Thailand in 2017: During April, May, and June, China Telecom hijacked routes from Italy to a financial company in Thailand.

Freedom on the Net 2018 – The Rise of Digital Authoritarianism
Freedom House (October 2018)

https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism
"In January 2018, African Union security staff reported that their computer systems had been sending confidential data back to Shanghai every day for five years … China had spent $200 million constructing the AU's new headquarters in Addis Ababa, including its computer network."

Chinese-Authored Spyware Found on More Than 700 Million Android Phones
By Chris Bing
Cyberscoop (Nov. 15, 2016)
https://www.cyberscoop.com/android-malware-china-huawei-zte-kryptowire-blu-products/
"More than 700 million Android phones, some of which were used in the U.S., carried hidden software than enabled surveillance by tracking user's movements and communications, a Virginia-based team of security researchers found."

"The firmware, discovered by Kryptowire, was reportedly authored by Chinese startup Shanghai Adups Technology company … The researchers discovered that Adups' firmware transmitted data packers to a Chinese server every 72 hours. These packets contained users call logs, text messages, contact lists, GPS location and other data."

"BLU products, an American phone manufacturer, told the New York Times that 120,000 of its phones were affected and that a subsequent software update would eliminate the surveillance feature."

b. Chinese Companies in Europe

We Should Worry About How China Uses Apps Like TikTok
Illiberal innovations created for China's vast surveilled and censored domestic market are increasingly popular overseas.
By Nick Frisch
New York Times - Opinion (May 2, 2019)
https://www.nytimes.com/interactive/2019/05/02/opinion/will-china-export-its-illiberal-innovation.html
"TikTok itself has already been fined by the Federal Trade Commission for a casual attitude toward privacy compliance; its heavy-handed solution, mass deletions, enraged some consumers. But the choices of ByteDance, TikTok's parent company, are rational; it fears the Communist Party more than angry tweets from tweens outside the Great Firewall."

Huawei AI Could Power Self-Driving Cars in Europe and China by 2021
By Echo Huang
Quartz (June 13, 2019)
https://qz.com/1642586/huawei-ai-could-power-self-driving-cars-in-europe-china-by-2021/
"The Chinese telecoms giant [Huawei] is looking to ship a self-driving car using its own AI technology in 2021 or 2022, Huawei's chief strategy architect Dang Wenshuan told the Financial Times June 12. Huawei is providing its AI infrastructure to a number of high-profile carmakers, including Audi, and China's state-owned carmakers, GAC Group, Beijing New Energy

Automobile, and Changan Automobile. Dang said the first self-driving cars are likely to come from Chinese manufacturers, but they will be available in both Europe and China."

WeChat Pay Eyes Europe for Cross-Border Business
By Alara Basul
UKTN (May 20, 2019)
https://www.uktech.news/news/wechat-pay-eyes-up-europe-for-cross-border-business-20190520
"WeChat Pay has announced that Europe will be the next key market for WeChat Pay Cross-border Business. As of April 2019, the number of merchants in the European region offering WeChat Pay as a payment method was 3.5 times higher than the previous year. WeChat has 1.112 billion monthly active users worldwide, of which 800 million are users of WeChat Pay. WeChat Pay has officially entered more than 49 overseas countries and regions, making it an excellent way for global merchants to quickly and effectively connect with Chinese tourists."

Alibaba to open first e-commerce trade hub in Europe
By Arjun Kharpal
CNBC (Dec. 5, 2018)
https://www.cnbc.com/2018/12/05/alibaba-to-open-first-e-commerce-trade-hub-in-europe.html
"Belgium is the first European country to sign up to the Electronic World Trade Platform (eWTP), an initiative first proposed by Alibaba co-founder Jack Ma in 2016. The plan is to help small-and-medium-sized enterprises to sell products abroad, something they have traditionally found complicated and expensive. As part of the initiative, Alibaba is opening a warehouse under its logistics arm Cainiao in Liege, Belgium. This will help businesses in Europe transport goods to China."

Freedom on the Net 2018 – The Rise of Digital Authoritarianism
Freedom House (October 2018)
https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism
"China remakes the world in its techno-dystopian image …Chinese firms also provided high-tech tools of surveillance to governments that lack respect for human rights … As more of the world's critical telecommunications infrastructure is built in China, global data may become more accessible to Chinese intelligence agencies."

Alibaba Expands Cloud Business to U.K. With New Data Centers
By Nate Lanxon and Thomas Seal
Bloomberg (Oct. 22, 2018)
https://www.bloomberg.com/news/articles/2018-10-22/alibaba-expands-cloud-business-to-u-k-with-new-data-centers
"The cloud-computing arm of Chinese retail giant Alibaba Group Holding Ltd. opened its first data centers in the U.K., with two sites operational in London. The expansion is 'driven by the rapidly growing customer demand,' a spokesman for the company told Bloomberg. 'The United Kingdom is one of the fastest-growing European markets for Alibaba Cloud.'"

Alibaba launches A.I., big data cloud products in Europe in challenge to Amazon, Microsoft
By Arjun Kharpal

CNBC (Feb. 27. 2018)
https://www.cnbc.com/2018/02/27/alibaba-cloud-expands-products-in-europe-to-take-on-amazon-microsoft.html
"Alibaba Cloud has been in Europe since 2016, and last year launched another AI and data-focused product into the market. But so far, Alibaba's efforts have focused on serving Chinese customers operating in Europe. Now it wants to try and sign up European businesses."

WeChat's Privacy Issues Mean You Should Delete China's No. 1 Messaging App
By Angus Grigg
Financial Review - Opinion (Feb, 22, 2018)
https://www.afr.com/news/world/asia/wechats-privacy-issues-mean-you-should-delete-chinas-no1-messaging-app-20180221-h0wgct
"Tencent and [Chinese internet giant] Alibaba are collecting a ton of information for their own commercial use, but this also dovetails nicely with what the Communist Party wants … This leaves many Australians with an age-old China dilemma – is the price of engaging with the country worth what may have to be given up? The dilemma is made all the more difficult as business, media, academic and government delegations are often asked to download WeChat when they first arrive in China by their local handlers, so the group can stay in touch."

WeChat confirms that it makes all private user data available to the Chinese government
WeChat, which is developed by Chinese firm Tencent, is a messaging app similar to Whatsapp
MoneyControl (Sept. 19, 2017)
https://www.moneycontrol.com/news/business/companies/wechat-confirms-that-it-makes-all-private-user-data-available-to-the-chinese-government-2391847.html
"WeChat has confirmed what has been rumoured all along i.e. it gives all user information to the Chinese government. The popular app in a privacy statement is now informing the users that virtually all the private user information will be disclosed to the authorities … A 2016 survey by Amnesty International ranked it lowest among popular messaging apps with regard to privacy protection of its users."

Chinese Internet Giant Tencent Launches WeChat Pay in Europe to Challenge Alibaba's Pay
By Arjun Kharpal
CNBC (July 10, 2017)
https://www.cnbc.com/2017/07/10/wechat-pay-europe-launch-tencent-to-challenge-alipay.html
"Tencent has partnered with German payments firm Wirecard to allow European retailers to accept WeChat pay as a payment option … Wirecard was also the company that helped Alipay launch in Europe in 2015."

Tencent Dominates China. Next Challenge is Rest of the World
By Brad Stone & Lulu Yilun Chen
Bloomberg Businessweek (June 28, 2017)
https://www.bloomberg.com/news/features/2017-06-28/tencent-rules-china-the-problem-is-the-rest-of-the-world

"Tencent is nearing market saturation in China and has to look elsewhere if it wants to continue to grow at the same torrid rate. He says that in 2013 he wanted to make a significant "strategic" investment in Snapchat but had to settle for investing a smaller amount."

SoftBank Group Corp., the Japanese tech conglomerate, was putting Finnish mobile game company Supercell Oy on the market… Tencent acquired a controlling interest in Supercell.

Big Brother collecting big data – and in China it's all for sale
By Sasa Petricic
CBS News (Jan. 11, 2017)
https://www.cbc.ca/news/world/china-data-for-sale-privacy-1.3927137
China maintains censorship controls and often gathers information when Chinese students study abroad and use certain applications, such as WeChat.

Baidu – the Google of China – Eyes Expansion to US, Europe: CEO
By Arjun Kharpal
CNBC (July 1, 2016)
https://www.cnbc.com/2016/07/01/baidu--the-google-of-china--eyes-expansion-to-us-europe-ceo.html
"Baidu – often dubbed the Google of China – will eventually expand into the U.S. and Europe, the Chinese search giant's chief executive said on Friday, as the business looks into new areas such as driverless cars and finance."

Government cyber-surveillance is the norm in China — and it's popular
The Washington Post - Opinion (Jan. 29, 2016)
https://www.washingtonpost.com/opinions/cyber-surveillance-is-a-way-of-life-in-china/2016/01/29/e4e856dc-c476-11e5-a4aa-f25866ba0dc6_story.html?noredirect=on&utm_term=.9a6c9b62a957
"China Mobile is the world's largest mobile phone company, with more than 800 million customers. To generate that automatic anti-fraud text message, international calls routed across the network in all likelihood pass through a server layer controlled and monitored by the PSB; calls from certain countries get flagged, and the text message is dispatched as the call is taking place."

"Upon landing on a trip to another country, I usually get an automatic Chinese-language text message from the Chinese Ministry of Foreign Affairs reminding me to behave politely and providing me with emergency contact numbers … The system then generates the text welcoming the user to that country and populating the message with the number for the nearest Chinese embassy and consulate."

European Airlines Take Alipay, WeChat Wallet
AirFrance
https://www.airfrance.com.cn/CN/en/local/resainfovol/achat/moyens-de-paiement.htm

Lufthansa
https://www.lufthansa.com/am/en/methods-of-payment

https://apex.aero/2018/04/04/lufthansa-systems-optile-payment

c. Chinese Market Share in Europe

Huawei, 5G Wireless, and the Battle for Europe
By Claude Barfield
AEIdeas (Feb. 25, 2019)
https://www.aei.org/publication/huawei-5g-wireless-and-the-battle-for-europe/?mkt_tok=eyJpIjoiTWpjd00yTTJaREE0T0daaSIsInQiOiJ6QWR4UzgxdmQ4V0NzWHFwRHFNbnpLdlNpeURLYXM0bG9FaDlMdUE5bUpBRWprc1ZLZ0VtUnhXVXBHM0g0NWQzd25xSldFaE82MlJvYVl6S0ErWEhiTTVIWmNKeDRvbGRLV0RZR1wvdW9ZXC9MazVUOUZVTWxkNThlXC9LcUZJQ0I0eSJ9
"…Huawei is strongly entrenched in the EU, where it boasts about a third of the European telecoms equipment market, with chief rivals Ericsson and Nokia each holding about one-fifth or slightly more of that market."

Chinese phones account for one-third market share in Europe
By Vlad Savov
The Verge (Feb. 14, 2019)
https://www.theverge.com/2019/2/14/18224614/huawei-chinese-phones-europe-market-share-2018
"… 32 percent, or roughly one-third, of smartphone shipments in Europe in 2018 were from Chinese manufacturers, with Huawei taking the lion's share of that with more than 23 percent of the overall market in the final months of the year."

German ambassador Michael Clauss on relations with China, the challenges and potential
South China Morning News (Dec. 22, 2017)
https://www.scmp.com/news/china/diplomacy-defence/article/2125328/german-ambassador-michael-clauss-relations-china
"Bilateral trade volume [between Germany and China] has risen to €170 billion (US$201.54 billion) in 2016 and further increased by 11 per cent in the first eight months of this year. China is Germany's top trading partner in the world."

European Trading Partners
Germany –
Exports to China – 7.1% Exports to U.S. – 8.4%
Imports from China – 10.0% Imports from U.S. – 5.7%
https://atlas.media.mit.edu/en/profile/country/deu/

France –
Exports to China – 4.3% Exports to U.S. – 7.0%
Imports from China – 8.9% Imports from U.S. – 6.3%
https://atlas.media.mit.edu/en/profile/country/fra/

Spain –

Exports to China – 2.5%	Exports to U.S. – 4.8%
Imports from China – 8.6%	Imports from U.S. – 4.5%

https://atlas.media.mit.edu/en/profile/country/esp/

3. China lacks rule-of-law safeguards against excessive surveillance, and personal data held by companies in China is accessible to the government.

The third theme of the research is that China lacks rule-of-law safeguards against excessive surveillance, and personal data held by companies in China is accessible to the government.

This document organizes the lack of safeguards in China based on a 2014 issue of International Data Privacy Law by Ira Rubinstein, Gregory Nojeim and Ronald Lee, cited in full below. The researchers compiled a normative framework to measure how national rules measured up against the standards for surveillance identified by the European Court of Human Rights. Unlike almost every other country surveyed, China lacked laws consistent with the 14 standards below for real-time surveillance in criminal investigations. 14 standards identified in the normative framework: 1. "in accordance with law;" 2. court order; 3. approval of senior official; 4. limited to serious crimes or threats; 5. particularity as to target; 6. showing of suspicion; 7. exhaustion of less intrusive means; 8. limit on duration; 9. limit on scope; 10. limit on use and disclosure; 11. retention limit/limit on storage; 12. notice to target; 13. oversight by independent entity; and 14. redress (remedy).

a. Safeguards – Democracy and the Rule of Law

Freedom on the Net 2018 – The Rise of Digital Authoritarianism
Freedom House (October 2018)
https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism
"China was once again the worst abuser of internet freedom in 2018." The ranking is based on the score from three categories: a) obstacles to access; b) limits on content; and c) violations of user rights. The category of violations of user rights is defined as follows: "Measures legal protections and restrictions on online activity; surveillance; privacy; and repercussions for online activity, such as legal prosecution, imprisonment, physical attacks, and other forms of harassment."

Systemic Government Access to Personal Data: A Comparative Analysis
By Ira Rubinstein, Gregory Nojeim & Ronald Lee
International Data Privacy Law (2014)
https://academic.oup.com/idpl/article/4/2/96/734798
The report surveyed 13 countries – Australia, Brazil, Canada, China, France, Germany, India, Israel, Italy, Japan, South Korea, the United Kingdom, and the United States.
China "explicitly carves out broad exceptions for national security from both the constitution and relevant security and surveillance laws." "China stands out among the 13 countries surveyed in two fundamental respects: first, it is the only non-democratic country; second, its constitution (and laws) grant extensive surveillance powers to the state for purposes of national and public security."

The researchers compiled a normative framework to measure how national rules measured up against the standards for surveillance identified by the European Court of Human Rights. Unlike almost every other country surveyed, China lacked laws consistent with the 14 standards below for real-time surveillance in criminal investigations. 14 standards identified in the normative framework: 1. "'in accordance with law;'" 2. "court order;" 3. "approval of senior official;" 4. "limited to serious crimes or threats;" 5. "particularity as to target;" 6. "showing of suspicion;" 7. "exhaustion of less intrusive means;" 8. "limit on duration;" 9. "limit on scope;" 10. "limit on use and disclosure;" 11. "retention limit/limit on storage;" 12. "notice to target;" 13. "oversight by independent entity;" and 14. "redress (remedy)."

"China meets none of the 14 standards identified in the normative framework."

The Data Protection Regime in China: In-Depth Analysis for the LIBE Committee
By Paul de Hert & Vagelis Papakonstantinou
European Parliament Directorate General for Internal Policies (Oct. 2015)
http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf
"[A]s far as its political regime is concerned, China is an authoritarian state that is governed by the China's Communist Party. With regard to the rule of law, while noteworthy modernisation attempts have been noted particularly in the past few years, it has also been noted that, for the time being, China is a country where 'the concept of rights is so weakly established and the rule of law is hostage to politics.'"

"While assessing the Chinese approach to data protection, the basic terms of reference of any relevant instrument ought to be kept in mind: (a) Human rights, at least as known in western countries, are not protected in China, (b) The public sector, and all state aims and purposes as dynamically defined by China's ruling Communist Part from time to time, should generally be perceived as exempted from all legislation, and (c) Court decisions do not lead to legal certainty."

Systematic government access to private-sector data in China
By Zhizheng Wang
International Data Privacy Law, Vol. 2, No. 4 (2012)
https://academic.oup.com/idpl/article/2/4/220/676863
"China was indeed 'in transition toward rule of law but still falling short of the minimal standard of achievement required to be considered rule of law' ten years ago and the situation remains much the same now—and will not be much changed in the forseeable future under the current political system of this one party socialist state unless substantial political reform takes place."

b. Safeguards – Independent Judiciary[2]

[2] Note to the reader: the safeguards are those listed in the normative framework based on the European Court of Human Rights. The title of the sub-section might thus be understood as "*Lack of* safeguards – independent judiciary."

Apple Moves to Store iCloud keys in China, Raising Human Rights Fears
By Stephen Nellis and Cate Cadell
Reuters (Feb. 24, 2018)
https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060
"Apple said it will only respond to valid legal requests in China, but China's domestic legal process is very different than that in the U.S., lacking anything quite like an American 'warrant' reviewed by an independent court, Chinese legal experts said. Court approval isn't required under Chinese law and police can issue and execute warrants."

WeChat's Privacy Issues Mean You Should Delete China's No.1 Messaging App
By Angus Grigg
Financial Review (Feb. 22, 2018)
https://www.afr.com/news/world/asia/wechats-privacy-issues-mean-you-should-delete-chinas-no1-messaging-app-20180221-h0wgct
"China does not have the same level of judicial oversight as the US telcos and others around the world," said Fergus Ryan, a cyber security analyst at the Australian Strategic Policy Institute in Canberra, who has previously worked in China.

European Parliament Directorate General for Internal Policies
By Paul de Hert & Vagelis Papakonstantinou
European Parliament Directorate General for Internal Policies (Oct. 2015)
http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf
"The assessment of a Western-type human rights model against an Asian background is by no means an easy task, given the big differences in the cultures involved. This task is further burdened when the country in question is China, where the essential human rights' conditions (horizontal application, independent courts and legal certainty) are not in place."

Systemic Government Access to Personal Data: A Comparative Analysis
By Ira Rubinstein, Gregory Nojeim & Ronald Lee
International Data Privacy Law (2014)
https://academic.oup.com/idpl/article/4/2/96/734798
"Chinese government access to private sector data is further strengthened by the Chinese Communist Party's 'absolute control over the law' and the absence of an independent judiciary."

c. Safeguards – Limited Access by Government

Beijing's New National Intelligence Law: From Defense to Offense
By Murray Scot Tanner
Lawfare (July 20, 2017)
https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense
"Speaking to a teleconference shortly before the Intelligence Law's passage, one senior corporate cybersecurity specialist expressed concern that state security officials could simply show up at a firm's offices in Beijing, show their badges, and demand technical cooperation."

CBC Highlights Citizen Lab Research on China
By Amitpal Singh
The Citizen Lab (Jan. 13, 2017)
https://citizenlab.ca/2017/01/cbc-article-chinese-censorship-highlights-citizen-lab-research/
Chinese officials "have a wealth of data at their disposal about what individuals are doing at a micro level in ways that they never had before. What the government has managed to do … is download the controls to the private sector, to make it incumbent upon them to police their own networks." It appears China stores "massive amounts of user data indefinitely."

U.S., Japan, EU team up to warn China of concerns over new security laws
The Guardian (Reuters) (Feb. 29, 2016)
https://www.theguardian.com/world/2016/mar/01/us-japan-eu-team-up-to-warn-china-of-concerns-over-new-security-laws
"The US, Canadian, German and Japanese ambassadors signed a letter addressed to minister of public security Guo Shengkun, voicing unease about the new and draft laws [on cyber security and counterterrorism]."

"In what sources said was a coordinated move, the ambassador of the European Union delegation to China, Hans Dietmar Schweisgut, sent a letter expressing similar concerns."
"The cyber security and counterterrorism laws codify sweeping powers for the government to combat perceived threats, from widespread censorship to heightened control over certain technologies."

Systemic Government Access to Personal Data: A Comparative Analysis
By Ira Rubinstein, Gregory Nojeim & Ronald Lee
International Data Privacy Law (2014)
https://academic.oup.com/idpl/article/4/2/96/734798
The report surveyed 13 countries – Australia, Brazil, Canada, China, France, Germany, India, Israel, Italy, Japan, South Korea, the United Kingdom, and the United States.
"Governments around the world have always demanded that commercial entities disclose data about their customers in connection with criminal investigations, enforcement of regulatory systems, and national security matters … The Chinese government maintains almost unlimited and unfettered access to private sector data, through a variety of regulatory requirements."
China does not require a court order for surveillance in criminal investigations. Location can be tracked without a warrant in China. China does not limit use, retention, or disclosure.

"Standards for real-time interception of communications for law enforcement purposes are high in most countries surveyed" but not in China. "Real-time surveillance is addressed in the majority of countries (other than China and India) in surveillance laws whose principles and concepts generally fit within the descriptive and normative frameworks outlined above. Against this commonality of approach, China and India stand out among the 13 countries surveyed. In China, it is very easy to override existing statutory restrictions on national security or public order grounds. Thus, Chinese law explicitly authorizes governmental access to privately held data and/or lacks explicit limitations on such access. Indeed, Chinese national security law

allows for the inspection of electronic communication instruments belonging to 'any organization or individual' for purposes of state security with few if any limitations." China's government "has extensive authorities and 'generous room for flexibility' in accessing private data in the name of maintaining state security and the social order."

d. Safeguards – Clear and Precise Rules

Beijing's New National Intelligence Law: From Defense to Offense
By Murray Scot Tanner
Lawfare (July 20, 2017)
https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense
"Like other recent Chinese security legislation, the Intelligence Law leaves key concepts undefined, thereby expanding the law's potential scope and its risks to foreigners. Most importantly, the law does not define its title concepts—"intelligence" or "intelligence work"—with details that clarify unacceptable government behavior or limit the obligations the law imposes on people and organizations."

"In this regard, a useful metric for comparison is one of the most fundamental of U.S. intelligence collection authorities, Executive Order 12333 on Intelligence Activities, which lays out detailed definitions, procedures, limitations and prohibitions regarding a number of intelligence activities, including government collection, retention, and dissemination of information on U.S. persons and corporations."

A Primer on China's New Cybersecurity Law: Privacy, Cross Border Transfer Requirements, and Data Localization
By Courtney Bowman, Ying Li, and Lijuan Hou
Proskauer Privacy Blog (May 9, 2017)
https://privacylaw.proskauer.com/2017/05/articles/international/a-primer-on-chinas-new-cybersecurity-law-privacy-cross-border-transfer-requirements-and-data-localization/
"[T]he vaguely-worded National Security Law, which has been called out by the UN High Commissioner for Human Rights for its 'extraordinarily broad scope,' permits the government to take 'all necessary' steps to guard China's sovereignty (including, it is speculated, by implementing wide-ranging surveillance measures). Meanwhile, the Anti-Terrorism Law requires telecom and Internet providers to allow access and grant other forms of assistance (such as decryption) to government authorities to prevent and investigate terror attacks."

Systematic Government Access to Personal Data: A Comparative Analysis
By Ira Rubenstein, Greg Nojeim, and Ronald Lee
Center for Democracy and Technology (Nov. 13, 2013)
https://cdt.org/files/2014/11/government-access-to-data-comparative-analysis.pdf
"In China, it is very easy to override existing statutory restrictions on national security or public order grounds. Thus, Chinese law explicitly authorizes governmental access to privately held data and/or lacks explicit limitations on such access. Indeed, Chinese national security law allows for the inspection of electronic communication instruments belonging to 'any organization or individual' for purposes of state security with few if any limitations … Comparative legal analysis is always difficult without an in--depth knowledge of the systems at

issue, and in the context of government access the task is made more difficulty [sic] by the ambiguity in laws and lack of transparency in practices."

e. Safeguards – Remedies

Europe Eyes Privacy Clampdown on China
A Global Standoff over Huawei and Chinese Surveillance is Prompting Europe to Question Whether its Data is Safe in China
Politico (February 12, 2019)
https://www.politico.eu/article/european-union-eyes-privacy-clampdown-on-china-surveillance-huawei/
"Commission officials stress that the intelligence and law enforcement regime in China does not pass the EU's standard for privacy protections, and that EU citizens would not have legal certainty when seeking redress before Chinese courts for privacy violations. That means that the EU would not sign an 'adequacy decision' with China, ruling out Europe's preferred mechanism to challenge excessive surveillance, the official said. In other words, China is unlikely to benefit from an overarching legal agreement like Privacy Shield, the current arrangement with the United States on data flows."

Beijing's New National Intelligence Law: From Defense to Offense
By Murray Scot Tanner
Lawfare (July 20, 2017)
https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense
"While the law requires that intelligence officials carry out such inquiries according to relevant state regulations, nowhere does the law explicitly authorize individuals or other actors whom they question—citizen or foreign—to refuse to answer questions or decline such access, information, or support. In this context, it is worth recalling that China's Criminal Procedure Law requires persons questioned by law enforcement officials (including public security officials) to respond "according to the facts" and does not confer on them the right to silence. What is unclear is whether the passage of the Intelligence Law effectively places these intelligence activities within the same realm as criminal cases, which might compel persons who are interviewed to cooperate with intelligence officials."

"Under the Intelligence Law, corporations could file complaints if intelligence agencies exceed their legal authority, although they may be limited to complaining to the agencies themselves. But the law says nothing about procedures for staying an improper demand for intelligence assistance or for filing lawsuits (in contrast, many recent lawsuits have been filed in U.S. federal courts by corporations and foundations challenging intelligence information requests, National Security Letters, and their confidentiality clauses)."

"Of special concern are signs that the Intelligence Law's drafters are … creating affirmative legal responsibilities for Chinese and, in some cases, foreign citizens, companies, or organizations operating in China to provide cooperation, or support for Beijing's intelligence-gathering activities."

f. Safeguard – Oversight

Europe Eyes Privacy Clampdown on China
A Global Standoff over Huawei and Chinese Surveillance is Prompting Europe to Question Whether its Data is Safe in China
Politico (February 12, 2019)
https://www.politico.eu/article/european-union-eyes-privacy-clampdown-on-china-surveillance-huawei/
"Every intelligence service should spy, by default. Otherwise it wouldn't be effective … The question is to whom they report and what is predictable and proportionate," said Giovanni Buttarelli, the EU's privacy watchdog.

What You Need to Know about China's Intelligence Law that Takes Effect Today
Quartz Staff
Quartz (June 28, 2017)
https://qz.com/1016531/what-you-need-to-know-about-chinas-intelligence-law-that-takes-effect-today/
The new intelligence law gives intelligence agencies "legal ground to carry out their work both inside and outside of China." "It is unclear how much legal oversight Chinese intelligence agencies are subject to."

Systemic Government Access to Personal Data: A Comparative Analysis
By Ira Rubinstein, Gregory Nojeim & Ronald Lee
International Data Privacy Law (2014)
https://academic.oup.com/idpl/article/4/2/96/734798
The report surveyed 13 countries – Australia, Brazil, Canada, China, France, Germany, India, Israel, Italy, Japan, South Korea, the United Kingdom, and the United States.
"Each country except China has some process of independent oversight of surveillance and government access."

With regard to protections, China is a standout "due to an almost total lack of protection and oversight in both law enforcement and national security."

4. By contrast with China, the United States has longstanding and extensive safeguards against excessive government surveillance.

The fourth theme of the research is that, by contrast with China, the United States has longstanding and extensive safeguards against excessive government surveillance.

The documents listed here document significant such safeguards for the U.S., using the same list of 14 standards used in Part 3, with respect to China's lack of safeguards.

a. Safeguards – Democracy and the Rule of Law

Freedom on the Net 2018 – The Rise of Digital Authoritarianism
Freedom House (October 2018)
https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism
The U.S. ranked sixth in internet freedom. In order, the top countries ranked as follows: Iceland, Estonia, Canada, Germany, Australia, and the U.S. The ranking is based on the score from three categories: a) obstacles to access; b) limits on content; and c) violations of user rights. The category of violations of user rights is defined as follows: "Measures legal protections and restrictions on online activity; surveillance; privacy; and repercussions for online activity, such as legal prosecution, imprisonment, physical attacks, and other forms of harassment."

Professor Peter Swire Testimony in Irish High Court Case
By Peter Swire
Alston & Bird (Nov. 2, 2017)
https://www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony
"Four features of the US system of government [include]: (1) a time-tested system of checks and balances; (2) judicial independence; (3) constitutional protection of individual rights; and (4) democratic accountability."

In the testimony, these safeguards are detailed in Chapter 3: Systemic Safeguards in Foreign Intelligence Surveillance Law and Chapter 4: Systemic Safeguards in Criminal Law.

How Both the EU and the U.S. are 'Stricter' than Each Other for the Privacy of Government Requests for Information
By Peter Swire and DeBrae Kennedy-Mayo
Emory Law Journal (2017)
http://law.emory.edu/elj/_documents/volumes/66/3/swire-kennedy-mayo.pdf
"Numerous safeguards concerning government access to information arise from the structure of government in the United States, as a constitutional democracy under the rule of law."

U.S. Surveillance Law, Safe Harbor, and Reforms Since 2013
By Peter Swire
Presented before the Belgium Privacy Authority's Forum on "The Consequences of the Judgment of the Schrems Case" (Dec. 18, 2015)
https://peterswire.net/wp-content/uploads/Schrems-White-Paper-12-18-2015.pdf

"The US Congress and executive branch have instituted two dozen significant reforms to surveillance law and practice since 2013."

These reforms are detailed in the testimony before the Belgium Privacy Authority.

b , Safeguards – Independent Judiciary

Professor Peter Swire Testimony in Irish High Court Case
By Peter Swire
Alston & Bird (Nov. 2, 2017)
https://www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony
"Standard practice in the US is that search warrants are issued by a judge, who is a member of the judiciary and not part of the executive branch. Federal judges have strong legal guarantees of independence – Article III of the US Constitution guarantees that federal judges have lifetime tenure, and cannot have their salaries reduced."

In the testimony, these safeguards are detailed in Chapter 3: Systemic Safeguards in Foreign Intelligence Surveillance Law and Chapter 4: Systemic Safeguards in Criminal Law.

How Both the EU and the U.S. are 'Stricter' than Each Other for the Privacy of Government Requests for Information
By Peter Swire and DeBrae Kennedy-Mayo
Emory Law Journal (2017)
http://law.emory.edu/elj/_documents/volumes/66/3/swire-kennedy-mayo.pdf
"The judiciary is a separate branch of government in the United States, established by Article III of the Constitution."

c. Safeguard – Limited Access by Government

Professor Peter Swire Testimony in Irish High Court Case
By Peter Swire
Alston & Bird (Nov. 2, 2017)
https://www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony
The U.S. legal system contains systemic safeguards in foreign intelligence surveillance law and systemic safeguards in criminal law.

In the testimony, these safeguards are detailed in Chapter 3: Systemic Safeguards in Foreign Intelligence Surveillance Law and Chapter 4: Systemic Safeguards in Criminal Law.

How Both the EU and the U.S. are 'Stricter' than Each Other for the Privacy of Government Requests for Information
By Peter Swire and DeBrae Kennedy-Mayo
Emory Law Journal (2017)
http://law.emory.edu/elj/_documents/volumes/66/3/swire-kennedy-mayo.pdf

"Consistent with constitutional requirements, the U.S. system provides numerous limits on law enforcement investigations … including: (1) oversight of searches by independent judicial officers; (2) probable cause of a crime as a relatively strict requirement for both physical and digital searches; (3) even stricter requirements for government use of telephone wiretaps and other realtime interception; (4) the exclusionary rule, preventing prosecutors' use of evidence that was illegally obtained, is supplemented by civil suits; (5) other legal standards that are relatively strict for government access in many nonsearch situations, such as the judge-supervised "reasonable and articulable suspicion" standard under ECPA; (6) transparency requirements, such as notice to the service provider of the legal basis for a request; (7) lack of data retention requirements for Internet communications; and (8) lack of limits on use of strong encryption."

"Independent federal judges play the central role in overseeing government surveillance requests, and those judges have access in the Foreign Intelligence Surveillance Court (FISC) to the classified information necessary for assessing government requests."

d. Safeguard – Clear and Precise Rules

Professor Peter Swire Testimony in Irish High Court Case
By Peter Swire
Alston & Bird (Nov. 2, 2017)
https://www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony
"[M]ajor safeguards in the US system of foreign intelligence law are codified in a number of statutes. The democratically-elected branches in the US have authorized surveillance to protect national security. They also have responded to evidence of excessive surveillance with laws setting limits on surveillance powers."

In the testimony, these safeguards are detailed in Chapter 3: Systemic Safeguards in Foreign Intelligence Surveillance Law and Chapter 4: Systemic Safeguards in Criminal Law.

How Both the EU and the U.S. are 'Stricter' than Each Other for the Privacy of Government Requests for Information
By Peter Swire and DeBrae Kennedy-Mayo
Emory Law Journal (2017)
http://law.emory.edu/elj/_documents/volumes/66/3/swire-kennedy-mayo.pdf
The Electronic Communications Privacy Act (ECPA) has been interpreted to require a probable cause warrant for access to "content of communications, including e-mails."
"The Foreign Intelligence Surveillance Act of 1978 (FISA) creates a comprehensive legal system for foreign intelligence surveillance."

e. Safeguards – Remedies

Professor Peter Swire Testimony in Irish High Court Case
By Peter Swire

Alston & Bird (Nov. 2, 2017)
https://www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony
"In the US, an EU resident or other individual has multiple remedies available for violations of privacy. These individual remedies work in tandem with the systemic safeguards."

In the testimony, these safeguards are detailed in Chapter 7: Individual Remedies in U.S. Privacy Law and Chapter 8: Individual Remedies, Hostile Actors, and National Security Considerations.

How Both the EU and the U.S. are 'Stricter' than Each Other for the Privacy of Government Requests for Information
By Peter Swire and DeBrae Kennedy-Mayo
Emory Law Journal (2017)
http://law.emory.edu/elj/_documents/volumes/66/3/swire-kennedy-mayo.pdf
"U.S. criminal law provides individual remedies to address evidence obtained during a search that was illegally conducted. In a criminal trial in the United States, the courts enforce constitutional rights by excluding evidence that the government obtains illegally. In addition, the courts bar evidence that is 'the fruit of the poisonous tree'—additional evidence similarly cannot be used in court if it is derived from an illegal search."

"With regard to civil remedies, an individual who has been the subject of a search that violated the Fourth Amendment can file a lawsuit suit seeking monetary damages. When the law enforcement officials conducting the search are state or local employees, the individual files a civil rights suit pursuant to 42 U.S.C. § 1983."

f. Safeguards – Oversight

Professor Peter Swire Testimony in Irish High Court Case
By Peter Swire
Alston & Bird (Nov. 2, 2017)
https://www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony
The testimony discusses "three paths of non-judicial remedies any individual in the US or EU can take: the Privacy and Civil Liberties Oversight Board, Congressional committees, and recourse to the US free press and privacy-protective nongovernmental organizations."
In the testimony, these safeguards are detailed in Chapter 3: Systemic Safeguards in Foreign Intelligence Surveillance Law and Chapter 4: Systemic Safeguards in Criminal Law.

How Both the EU and the U.S. are 'Stricter' than Each Other for the Privacy of Government Requests for Information
By Peter Swire and DeBrae Kennedy-Mayo
Emory Law Journal (2017)
http://law.emory.edu/elj/_documents/volumes/66/3/swire-kennedy-mayo.pdf
For criminal cases, the "[s]tandard practice in the United States is that search warrants are issued by a judge, who is a member of the judiciary, separate from the executive branch."

"There is a comprehensive oversight system for foreign intelligence, including Senate and House intelligence committees, agency inspectors general, privacy offices in executive agencies, and the independent Privacy and Civil Liberties Oversight Board."

5. Allowing data transfers to China while blocking them to the U.S. would be legally unjust and would cause large and negative consequences.

As discussed in the Le Monde article, allowing data transfers to China while blocking them to the U.S. would be legally unjust and would cause large and negative consequences.

Part 5 provides documents that discuss implications of a CJEU decision in the standard contract clauses case that affects only the U.S. and then more broadly. The most detailed written treatment is Peter Swire's expert report submitted on November 2, 2016 to the Irish High Court in the case where Max Schrems is challenging whether transfers of personal data under standard contract clauses are adequately protected under European Union privacy law. Under Irish rules, Swire was an expert selected by Facebook but required to give his independent opinion about U.S. law; Swire retained complete editorial control over the content of the testimony. Swire has played no role in the litigation since providing his expert testimony.

Only US:

Professor Peter Swire Testimony in Irish High Court Case
By Peter Swire
Alston & Bird (Nov. 2, 2017)
https://www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony
Professor Peter Swire, in his testimony to the Irish High Court in Schrems I (Data Protection Commissioner v. Facebook, Max Schrems), noted the economic effects of a finding that US lacks adequacy due to its surveillance regime. Swire discussed EU statements about the importance of the transatlantic economic relationship.

"The Privacy Shield documents state: "The transatlantic economic relationship is already the world's largest, accounting for half of global economic output and nearly one trillion dollars in goods and services trade, . . . supporting millions of jobs on both sides of the Atlantic."… Concerning data flows, the Commission's final Privacy Shield Adequacy Decision states that "the exponential increase in data flows" between the EU and the US is of "critical importance for the transatlantic economy."

In its review of the draft Privacy Shield documents, the European Data Protection Supervisor stated that the EU-US alliance is "the biggest trading partnership in the world," and that the purpose of its review was "to boost transatlantic relations" so that they could be "stable in the long term." … The Article 29 Working Party, while expressing concerns about aspects of the Privacy Shield, agreed that "data transfers that take place between the EU and the U.S. on a daily basis" constitute "a vital part of the economy on both sides of the Atlantic."

Non-EU (including China):

Professor Peter Swire Testimony in Irish High Court Case
By Peter Swire
Alston & Bird (Nov. 2, 2017)

https://www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony
Swire discussed the implications of a finding that US surveillance safeguards are inadequate, on trade with other countries, including BRIC countries. Swire points out that the General Agreement on Trade in Services (GATS) supports free trade and free transfer of data. Though there is a privacy exception, which permits the adoption of measure for protection of privacy of individuals, the exception is limited and subject "to the requirement that such measures are not applied in a manner which would constitute *a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail*, or a disguised restriction on trade in services."

In his view, GATS language provided an "additional reason to consider how the safeguards in the US compare to both the EU and to other nations, such as the BRIC countries … [T]he concern about "unjustifiable discrimination" would appear to apply if transfers were allowed to the BRIC or other countries but not to the US."

"The four BRIC countries are large and important nations and trading partners of the EU. All have extensive surveillance activities with less transparency and oversight, and fewer overall systemic safeguards and individual remedies, than the US."

"A categorical finding of inadequacy of US surveillance safeguards thus raises the risk of significant economic effects because of the elimination of lawful transfers, which according to EU institutions are vitally important, and also because of the sanctions that may result from treaty violation under the GATS."

Additional Commentary:

EU High Court Hearings to Determine Future of Privacy Shield, SCCs
By Jennifer Baker
IAPP Privacy Advisor (June 25, 2019)
https://iapp.org/news/a/eu-high-court-hearings-to-determine-future-of-privacy-shield-standard-contractual-clauses/?mkt_tok=eyJpIjoiWkdaalpEWmlOalk0WmpCbCIsInQiOiJ5N0RmakhqcGw2V0N5MlJzVDhCcTk4azZ1QTYreG9tY3VxRlJhV0NsRndKOXRhVmdFcTM4djhjZzVqWWZHNG16RmpsdU1SbmRHMUxDMWpkcXRZOGt3T3N5MURPenhwSWxNdFRHSHJiQV11WndcL2pnelFCVStvUmxxZWRXYzI4dnoifQ%3D%3D
"I think we are going to see some real panic as the prospect of invalidation nears later this year," Eduardo Ustartan, partner at Hogan Lovells in the U.K., told The Privacy Advisor.
"The Privacy Shield has always been surrounded by a degree of uncertainty, but the SCCs have been around for nearly 20 years, so they are the bedrock of lawful data transfers," he added. "The idea that the most widely used mechanism to support something so essential to the digital economy may crumble is almost unthinkable, but we can be sure that the CJEU will not be distracted from its mission to determine whether the SCCs are effective at extending European data protection globally."

Fin.