Share Your News Now

If you would like to share news or information with our readers, please send the unique stories, business news organization events, and school news to us includinig your name and phone number in case more information is needed.

For news and information consideration, please send to News@scdaily.com
or contact
John Robbins **832-280-5815**
Jun Gai **281-498-4310**

# Southern DAILY
Make Today Different

Southern Daily News is published by Southern News Group Daily

**Publisher:** Wea H. Lee
**President:** Catherine Lee
**Editor:** John Robbins

**Address:** 11122 Bellaire Blvd., Houston, TX 77072
**E-mail:** News@scdaily.com

Trump-California rift widens as auto emissions talks fail

Inside C2



# ‘Tarnished image’: Myanmar touts troubled Rakhine as investment destination

YANGON (Reuters) - Organisers of a summit in Myanmar’s crisis-hit western state of Rakhine are this week pitching to investors its plentiful farmland and fishing grounds, tourist-ready beaches and historic temples.


A rider passes by the Rakhine State Investment Fair 2019 bulletin board in Ngapali beach in Thandwe, Rakhine State, Myanmar February 19, 2019. REUTERS/Ann Wang

The event’s website describes the “untouched opportunities” available in the strategically located region, close to large markets in India and Bangladesh. But a session at the fair will also be devoted to how to invest responsibly in the state, from which an estimated 730,000 minority Rohingya Muslims fled an army offensive in 2017.

A U.N. fact-finding mission last year said the military campaign, which refugees say included mass killings and rape, was orchestrated with “genocidal intent”. Myanmar denies the charge and says its offensive was a legitimate response to an insurgent threat and that it is welcoming the refugees back.

Myanmar hopes the Rakhine State Investment Fair – the first of its kind – will bring money into the impoverished region. Civilian leader Aung San Suu Kyi, who in the past has said economic development is the key to addressing the state’s long-standing religious and ethnic tensions, is scheduled to deliver the keynote speech on Friday.

Suu Kyi’s spokesman did not answer calls seeking comment.

Nobel laureate Suu Kyi last month pledged to make Myanmar more investment-friendly as she opened a separate investment summit in the capital, Naypyitaw.

But her government remains under pressure over the 2017 exodus of refugees to Bangladesh, and the plight of hundreds of thousands more Muslims still living in camps and villages inside Rakhine, where their movements and access to healthcare and education remain restricted. A separate conflict with Rakhine rebels that escalated in December has seen aid agencies blocked from reaching many areas.

“It’s quite extraordinary that this investment fair is on, even though large chunks of central Rakhine are now off limits to prying eyes,” said Laetitia van den Assum, a retired Dutch diplomat who was a member of a commission on Rakhine led by the late former U.N. chief Kofi Annan.

Southern DAILY Make Today Different

# WORLD NEWS

# Trump-California rift widens as auto emissions talks fail

WASHINGTON (Reuters) - U.S. federal officials have decided to end negotiations with California over the Trump administration's plans to roll back fuel economy rules designed to reduce greenhouse gas emissions, a government official said on Wednesday.

California and 19 other states have demanded the Trump administration abandon a proposal made in August to freeze fuel efficiency standards after 2020 and strip California of the ability to impose stricter rules.

Aside from the threat of increased pollution, Detroit automakers have the greatest financial interests at stake. General Motors, Ford Motor Co and Fiat Chrysler Automobiles generate most of their global profits from sales of fuel-thirsty large pickup trucks and sport utility vehicles in the United States. All three have discontinued or planned to drop small and medium-sized sedans from their lineups to focus on trucks and SUVs.

The rules to require automakers to roughly double average fuel efficiency by 2025 – with a corresponding decline in carbon dioxide emissions – were one of the Obama administration's most significant climate policy actions. Since taking office, Trump has worked to roll back a broad range of Obama environmental policies that were opposed by the oil and coal industries.

As the 2020 election cycle heats up, the fight over automotive emissions promises to be a dividing line between Trump and Democrats, many of whom are embracing a platform of aggressive action to curb climate emissions in what they call the Green New Deal.

Scrapping the talks also comes as power struggle between California and Trump grows. The Trump administration on Tuesday canceled $929 million in federal funds for a California high-speed rail project. California's governor quickly linked that move to California leading a 16 state coalition challenging Trump's national emergency to obtain funds for building a wall along the U.S.-Mexico border.

The California Air Resources Board (CARB), California's top clean air regulator, has been meeting with officials from the White House, U.S. Environmental Protection Agency and Transportation Department over Trump administration efforts to stop California from tightening vehicle emissions rules in the state.

The government official offered no further details on the end of the talks and it was not immediately clear when an announcement would be made.

California officials already have filed suit to block the Trump administration proposal to roll back federal fuel economy targets for 2022-2025. It is not clear how the industry would respond to the formal adoption of Trump's proposed freeze, and likely litigation by California and other states.

CARB Chair Mary Nichols last year said the state was willing to give automakers more flexibility to comply with vehicle greenhouse gas limits. EPA Administrator Andrew Wheeler and Nichols met two weeks ago in San Francisco but there were no substantive discussions, said CARB spokesman Stanley Young.

"The administration broke off communications before Christmas and never responded to our suggested areas of compromise — or offered any compromise proposal at all. We concluded at that point that they were never serious about negotiating," Young said.

Fuel tanks are shown in National City, California, U.S. June 27, 2018. REUTERS/Mike Blake

A source familiar with those discussions said EPA officials did not work on the rule during the government shutdown. "There was no real effort to get to yes," the source said.

Trump's EPA and the National Highway Traffic Safety Administration proposed a rule in August that would maintain emissions standards at 2020 levels rather than requiring that they improve.

Scientists have linked rising fossil fuel emissions to higher temperatures that have worsened drought conditions in California blamed for devastating fires.

California officials and environmental groups have said the Trump administration proposal would deal a blow to efforts to contain that damage.

Southern DAILY Make Today Different

# Editor's Choice

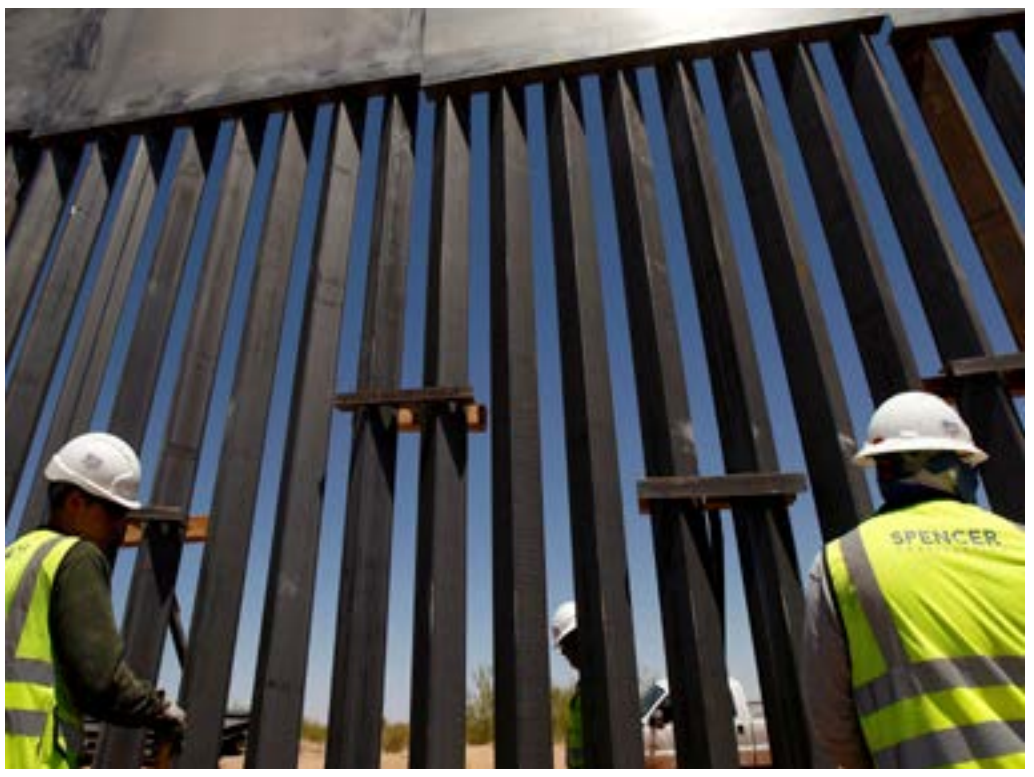
Migrants cross the Rio Bravo towards the United States, in Piedras Negras

Pink performs at the Brit Awards at the O2 Arena in London, Britain, February 20, 2019. REUTERS/Hannah McKay


FILE PHOTO: An illuminated sign appears in a Lyft ride-hailing car in Los Angeles

FILE PHOTO: FILE PHOTO: The prototypes for U.S. President Donald Trump's border wall are seen behind the border fence between Mexico and the United States, in Tijuana

The 1975 perform at the Brit Awards at the O2 Arena in London, Britain, February 20, 2019. REUTERS/Hannah McKay




FILE PHOTO: Construction workers check a new section of bollard wall in Santa Teresa as seen from the Mexican side of the border in San Jeronimo

Conservative leader Scheer receives a standing ovation during Question Period on Parliament Hill in Ottawa

American track and field sprinter Noah Lyles wears Sonic Hedgehog socks while training at the National Training Center in Clermont, Florida, U.S., February 19, 2019. REUTERS/Phelan Ebenhack

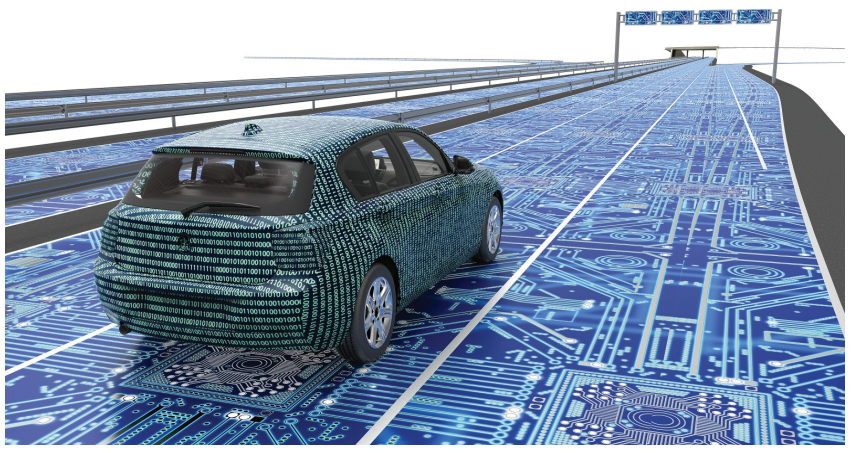
Southern DAILY Make Today Different

COMMUNITY

## *Carmakers Are Beefing Up Security Measures As Hackers Take Smart Cars For A Ride*

# Your High-Tech Car Is A Magnet For Hacking

**Compiled And Edited By John T. Robbins, Southern Daily Editor**



Hopping into an Uber or a Car2Go is a great way to get around. Unfortunately, hackers agree, exploiting weaknesses in apps to go on "phantom rides" with someone else's profile.

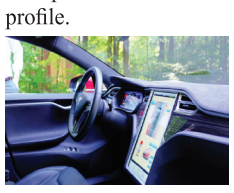
From such trips—like a man in Australia who went on more than 30 free drives on the GoGet car-sharing platform before being arrested—to vehicle theft and taking wireless control of cars, reported attacks on smart cars have ballooned six-fold over the past four years, according to research from cyber-security platform Upstream Security Ltd.

**Hacked Wheels**

As more cars connect to the web, cyberattacks go through the roof

While companies have taken note, with Daimler AG's Car2Go car sharing beefing up security measures after a limited number of accounts were hacked, risks around vehicle cybercrime are only going to get worse. Connected cars are forecast to double to 775 million by 2023, according to Juniper Research, enlarging the pool of convenience features like keyless entry, apps to turn on heating remotely and smartphone connection via bluetooth. "Each new service connected to a vehicle is a new potential entry point for hackers," Upstream wrote in a report published Monday. "Worst-case scenarios are loss to business earnings, theft, data privacy or property damage."

Hopping into an Uber or a Car2Go is a great way to get around. Unfortunately, hackers agree, exploiting weaknesses in apps to go on "phantom rides" with someone else's profile.



From such trips—like a man in Australia who went on more than 30 free drives on the GoGet car-sharing platform before being arrested—to vehicle theft and taking wireless control of cars, reported attacks on smart cars have ballooned six-fold over the past four years, according to research from cyber-security platform Upstream Security Ltd.

**Hacked Wheels**

As more cars connect to the web, cyberattacks go through the roof

While companies have taken note, with Daimler AG's Car2Go car sharing beefing up security measures after a limited number of accounts were hacked, risks around vehicle cybercrime are only going to get worse. Connected cars are forecast to double to 775 million by 2023, according to Juniper Research, enlarging the pool of convenience features like keyless entry, apps to turn on heating remotely and smartphone connection via bluetooth. "Each new service connected to a vehicle is a new potential entry point for hackers," Upstream wrote in a report published Monday. "Worst-case scenarios are loss to business earnings, theft, data privacy or property damage."

**Getting In**

Hackers target many weak spots in cars to gain access

Carmakers from Mercedes-Benz maker Daimler to Toyota Motor Corp. are pursuing digital services as potentially lucrative additional sources of revenue, as well as keeping pace with growing competition from the likes of Uber Technologies Inc. Daimler and BMW AG are in the process of combining their car-sharing platforms, to build a far broader suite of services including a ride-hailing app, electric-car charging and digital parking services.

Car-sharing platforms lack adequate protection, said cybersecurity and anti-virus provider Kaspersky Lab after testing 13 apps from Russia, the U.S. and Europe. Most of them allowed for weak passwords, didn't protect against reverse engineering, and failed to stop phishing attempts, according to a July report that didn't name the services tested.

**Valuable Access**

Controlling car systems, auto theft and data access are the main reasons for hacks

In the race to thwart cybercriminals, carmakers regularly invite software experts to test the robustness of their setups. While phantom rides are relatively harmless, hacks can be far more dangerous. In 2015, Fiat Chrysler Automobiles NV recalled 1.4 million cars and trucks after Wired magazine published a story about software programmers who were able to take over a Jeep Cherokee it was driven on a Missouri highway.

Uber, the ride-hailing app that's preparing a public share sale, says it has introduced security features like two-step log-in verification, since fraudsters in China used fake accounts to go on free rides.

"We have entire systems and organizations at Uber that are able to detect this kind of fraudulent activity," Uber told Bloomberg News in a statement. "Criminals will keep trying new ways to get what they want and we need to constantly respond to their evolving techniques. Fighting fraud never ends."

**The Industry Fights Back**

More sensors and software are going into cars all the time but that creates new security considerations.

**Why Are Cars Hackable?**

Why can cars be hacked? The reason is simple: They're filled with lots of software and connectivity. Brian Witten, Head of Advanced Technologies, Office of the CTO at Symantec, notes that potential attack vectors include cellular connectivity, as well as Bluetooth, WiFi, and more. In the United States, over a third [MOU1] of cars are already connected to the Internet.

Even if you don't have advanced features for streaming music or traffic updates to a navigation system, your car might still be connected to the Internet for simple automatic crash notification, saving lives.

A KPMG report, "Protecting the fleet… and the car business" notes, "The average car contains more than 150 million lines of code, plus multiple individual computers and a vast number of wireless connections to internal and external channels." It says that as a result, cars now have more code embedded in them than an F-25 fighter or a Boeing 787. It can seem almost impossible to protect automobiles, given their complex onboard systems and the logistics and money that would be required to fix all possible holes for millions of new and existing cars. A Symantec report, "Building Comprehensive Security into Cars," warns, "Companies often use redundancies at critical IT layers to keep high-volume web services running reliably, but few, if any, carmakers can afford the NASA-like investment of doing this for every vehicle."

**"Cars Today have more code embedded in them than an F-25 fighter or a Boeing 787"**

There are many potential incentives for hacking entire fleets. Imagine your car failing to start but displaying a number to which you need to wire money if you want your car to start. As such "automotive ransomware" risks become more likely, not all incentives are financial. For instance, foreign governments could do the hacking as part of a cyber attack on a nation's basic infrastructure.

**An F-25 fighter Jet.**

"Fleet hacking is a lot more tractable than a lot of people realize," Witten says.

Many people agree with him. Elon Musk believes it will be a particularly serious problem when autonomous vehicles become more widespread. "I think one of the biggest risks for autonomous vehicles is somebody achieving a fleet-wide hack," he said at the National Governors Association meeting last summer. The federal government has also started to take notice. The Department of Homeland Security (DHS) and the Department of Transportation (DoT) have been working on cyber security for the federal government's fleet of vehicles.

**What Can Be Done About It?**

What to do if you're worried about getting hacked? First, check to make sure that your car's software is updated by checking with the dealer. Many carmakers are in the process of fixing vulnerabilities in vehicle software.

Some are able to fix those vulnerabilities with updates sent "over the air" using the cellular network, but other automakers can only fix such vulnerabilities when the vehicle is brought in for regular maintenance.

Still, with so many attack vectors, nothing is perfect. In addition to cellular modems that are needed to save lives through Automatic Crash Notification (ACN), some of the risks to the vehicle might be in the supply chain itself.

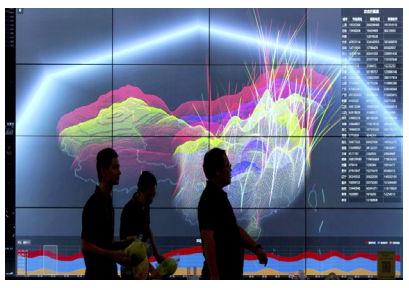

The answer, according to Witten, is that auto makers need to recognize the dangers of fleetwide hacking, and build wide-ranging security into cars, including a comprehensive security architecture, cryptographically protecting communications into and out of automobiles, working in concert with network operators who supply cars' connectivity, and building a vehicle security operations center where analysts can hunt security threats on at a fleetwide scale, and other systemwide protections.

"You've got to do all that, and also keep everything up to date, because security is never finished," he says. "The adversary is nimble, and if you're not agile, they are. And they're going to eat your lunch if you're not prepared." (Courtesy

Southern DAILY Make Today Different

# BUSINESS

SPECIAL REPORT



## China's Governance Of Cyberspace Still Evolving One Year After Crucial CSL Law Took Effect

# Progress, Pauses, and Power Shifts in China's Cybersecurity Law Regime

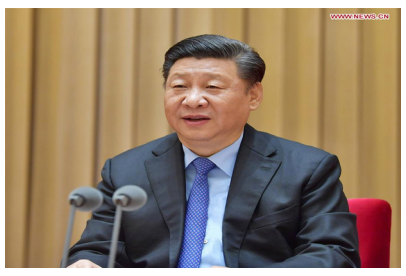
**Compiled And Edited By John T. Robbins, Southern Daily Editor**

China's Cybersecurity Law (CSL) has a remarkably wide reach in Chinese society, serving as the centerpiece of perhaps the most comprehensive cyberspace governance regime in the world. Still, more than a year after official implementation on June 1, 2017, a great deal of the regulatory and standards-setting work needed to give the law true force remains incomplete.

In policy areas including data localization, "critical information infrastructure" (CII) protection, and security reviews for "critical network equipment and specialized cybersecurity products," the CSL regime remains a work in progress. Personal information protection policies stand out as further along than others, but there is still more to do.

Passage of the CSL in November 2016 should therefore be seen not as an end result but as a major milestone in the broader "cybersecurity and informatization" push that the Xi Jinping leadership embarked on in 2014. The law enshrined high-level concepts and formulations, addressed turf battles among government offices, and put domestic and foreign stakeholders on notice that a broad definition of cybersecurity was a top Chinese government priority.

Amidst delays, top leaders appear to be demanding progress. In April, Xi personally chaired a national work conference on cybersecurity and informatization, where he gave a speech (coverage translated by DigiChina) that reiterated the Party's commitment to cybersecurity regulation and digital-driven development while clarifying some bureaucratic roles in the sector.



**Last April, China's President Xi personally chaired a national work conference on cybersecurity and informatization, where he gave a speech that reiterated the Party's commitment to cybersecurity regulation and digital-driven development.**

Moreover, the international circumstances China faces have changed considerably. The events surrounding the Chinese telecommunications equipment supplier ZTE and the escalating trade and investment confrontation with the United States have convinced Chinese officials that cybersecurity and technological development require strong and sustained attention. (Late last week the U.S. Commerce Department lifted a denial order on ZTE, which had prevented the company from purchasing hardware and software from U.S. suppliers.)

As regulatory and standards-setting efforts unfold with renewed vigor, several key areas of regulation have reached significant milestones, and others have run into bureaucratic and technical challenges.

Data Localization Rules Stall After U.S.- and Japanese-Led Pressure Campaign

The CSL explicitly requires certain types of data to be stored within mainland China, and it sets up conditions for transferring some types of data abroad. Two major draft regulatory documents released last year raised the specter of pervasive limits on cross-border transfer of data out of China. The draft documents—"Measures" and "Guidelines" on security reviews required for outbound transfer of "personal information" and "important data"—generated intense debate and international opposition.

Beginning in October 2017, the United States and Japan led a multilateral campaign against these draft rules at the WTO Council for Trade in Services, requesting that China refrain from issuing or implementing final measures until concerns were addressed and the draft regulations were fully consistent with the WTO General Agreement on Trade in Services. Under pressure from a broad coalition of trading partners, authorities suspended development of the Measures before U.S. President Donald Trump's November 2017 China visit, and they postponed work on the Guidelines in April 2018.

**The WTO Council for Trade in Services meeting in October 2017.**

Though the final resolution is uncertain, and the reviews for outbound data transfer are not slated to go into effect until the end of 2018, there are signs that restrictions may tighten rather than loosen compared with earlier drafts. The April Big Data Security Standardization White Paper 2018 included language that, if made binding, would expand the scope of checks on outbound data transfers to include datasets covering 500,000 people's data overall, rather than 500,000 per year.

Once the review regime for outbound data transfers is complete, companies will have a process to follow to move data in an approved way, including through internal assessments or hiring outside reviewers, according to the draft Measures. Regardless, for "personal information and important data" produced by operators of "critical information infrastructure" (see below), there remains a requirement to at minimum store a copy of the data in mainland China.

**Review Regimes Head Toward Greater Coordination**

The CSL establishes requirements for a regime to review "critical network equipment and specialized cybersecurity products" for security. In June, China's top certification organization, the Certification and Accreditation Administration of China (CNCA) announced 22 organizations in two lists as responsible for testing and certification in these areas. For the most part, these organizations are the designated testing or certification bodies in existing processes: for network access licenses under the Ministry of Industry and Information Technology (MIIT), for sales licenses or information security products under the Ministry of Public Security (MPS), etc. The approved bodies include a range of organizations with significant technical chops and experience reviewing foreign equipment.

A new name on the list comes in the form of the

Certification and Accreditation Administration of the People's Republic of China

newly renamed China Cybersecurity Review Technology and Certification Center (CCRTCC), whose director Wei Hao has played a public role in explaining the review process. Wei has said that review and certification efforts should be integrated to prevent duplication between existing processes and the new regime called for in the CSL, according to a WeChat post by the Critical Information Infrastructure Technology Innovation Alliance. In that post, Wei further described a national "data security review and certification system," and he ty and government cloud services, big data, etc."

Wei described the issuing of a catalog of "critical network equipment and specialized cybersecurity products" last year as the beginning of implementation of a national cybersecurity review system, and suggested that much more work needs to be done to clarify responsibilities and develop the new, more unified system.

**'Critical Information Infrastructure' (CII) Rules Vague in Early Drafts, but More Details Expected**

Under the CSL, operators of information systems in a broad and only partially defined array of sectors designated as "critical information infrastructure" (CII) may only purchase network products and services that have passed national security reviews that at present are set forth in trial measures. So far the national security review panel has approved six cloud platforms, all of which are operated by Chinese companies.

What sectors are to be covered by these rules remains unclear. In July 2017, the CAC published draft CII Security Protection Regulations for comment. That draft suggested a broad definition of CII, covering many sectors, but raised more questions than answers because it was not comprehensive. In a November 2017 meeting with global industry stakeholders, CAC Cybersecurity Coordination Department Director General Zhao Zeliang said he believed the scope of CII should be narrow, applying only to a small fraction of all information systems. Still, CAC would not set a deadline to finalize the definition of CII. An updated version of the draft regulations is expected in the coming weeks or months.

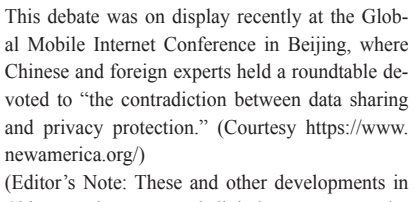
**Advantage CAC in Jurisdiction Overlap with Ministry of Public Security**


Even six months after CSL implementation, major questions remained regarding overlapping jurisdiction. (See DigiChina's earlier outline of six emerging systems.) The law set forth a new system for protecting CII, but it also reaffirmed an existing and inescapably overlapping system run by the MPS—the Multi-Level Protection Scheme (MLPS).

According to industry sources, MPS has been advocating that CAC repurpose the MLPS' cybersecurity requirements, rather than establishing a parallel regime for CII. CAC has insisted that its new system would not "conflict with, duplicate, modify, or lower the requirements set forth by the MLPS Baseline Requirements Standard."

Recent events suggest CAC's authority is increasingly clear in this area. On June 27 the MPS released the draft Cybersecurity Multi-Level Protection Regulation (MLPS 2.0 for short), an upgraded replacement of the original 2007 MLPS measures. The new document assigns primary regulatory leadership to the Central Commission for Cybersecurity and Informatization, CAC's recently elevated parent, seating it above MPS, which is designated a "competent authority." This proposed language suggests CAC will have the upper hand in settling divergent views regarding the boundary between rules for CII and the evolving MLPS.

Substantively, the draft MLPS 2.0 document would potentially cover companies that did not previously fall under the scope of MLPS by expanding the scheme to cover all network operators rather than just key industry systems or government agencies. In addition, it lowers the threshold for Level 3 status in the graded ranking, a level where requirements including enhanced monitoring by the MPS, third-party certification, and annual reviews kick in. There is an apparent shift toward more audits rather than self-reporting by companies.



**Protecting Personal Data a Particular Priority**

There has been an increasing emphasis on how personal information (PI) is managed in the year since the CSL took effect. The government has issued its first standard with granular rules for how personal data is collected, used, processed, and shared—the Personal Information Security Specification. The standard, though officially nonbinding, has already been cited by authorities targeting violations by major companies, including the Alibaba-linked Ant Financial.

The banking industry became the rare sector to issue its own guidelines for data governance in March. A statement by the China Banking Regulatory Commission linked the need for such measures to the massive amounts of client data now involved in core functions of financial institutions. Even the new MLPS 2.0 regime now stresses the importance of PI protection with seven separate articles addressing network operators who illegally leak, sell, or share PI without authorization.

Together these developments underscore a growing recognition that China needs some framework for personal data as part of the broader effort to govern China's digital economy and address citizen concerns about privacy.

Yet, implementation and enforcement of new PI rules is likely to be somewhat ad hoc and subject to political jockeying, because there is still much debate around data ownership, privacy, and the development of emerging technologies like AI. This debate was on display recently at the Global Mobile Internet Conference in Beijing, where Chinese and foreign experts held a roundtable devoted to "the contradiction between data sharing and privacy protection." (Courtesy https://www.newamerica.org/)

(Editor's Note: These and other developments in Chinese cyberspace and digital economy regulation represent a broad effort to manage the challenges and opportunities posed by digital technologies, a task that will never be fully complete.)