mlex
a LexisNexis company

DATA PROTECTION
SPECIAL REPORT
MAY 3, 2022

In an exclusive interview with MLex, South Korean privacy chief **Yoon Jong-in** discusses his agency's priorities and challenges — including keeping Big Tech in check, ushering in new privacy legislation and preparing for a world of automated cars.

Big Challenges Need Big Ideas

INSIGHT | COMMENTARY | ANALYSIS

Contents

INTERVIEW

By Wooyoung Lee & Jenny Lee

All stories first published on April 25, 2022

Photographs by Lee Jong-min for MLex

Wooyoung Lee is a senior correspondent based in MLex's Seoul office, covering antitrust, privacy and data security, mergers and acquisitions and financial services. Wooyoung has more than a decade of experience in journalism, public policy and research. She has worked and written for news outlets including The Korea Herald, Al Jazeera International, Bloomberg BNA, Monocle, among others. She worked as a foreign service officer for policy and research at the Ministry of Foreign Affairs of the Republic of Korea. She holds a BA in Linguistics from Kyunghee University and an MSc from the Sociology department of the London School of Economics and Political Science.

Jenny Lee joined MLex's Seoul bureau in 2021 as a correspondent focusing on competition law and data privacy and security. Jenny received a Master's degree from Northwestern University's renowned Medill School of Journalism and worked for a number of news organizations in the US, including the Associated Press Television News, McClatchy and Voice of America, where she worked for almost three years in Washington, DC. She returned to her native South Korea in 2019 as a reporter for Wired Korea.

Gargantuan enforcement tasks force South Korean privacy chief Yoon to hit the ground running

Yoon Jong-in, chairman of South Korea's new privacy watchdog, describes his experiences building the agency from scratch and setting the groundwork for the country's data-privacy rules, in an extended interview with MLex. He talks about goals, tasks and challenges facing the nascent agency, which involved countless hours of discussions and brainstorming sessions with stakeholders.

Despite a 30-year career in South Korea's public service, Yoon Jong-in had never imagined himself as the country's top privacy officer, nor had he expected to be chosen to build a government agency from scratch and provide the groundwork for the country's data-privacy rules.

Looking back, Yoon is happy to admit that the whirlwind experience that thrust him into the spotlight in 2020 was daunting.

The pressure was just overwhelming, Yoon told MLex in a recent interview. "I had to think about the expectations of the public as well as those of the president, prime minister and other relevant administrative bodies."

The weight of expectations from the wider population and the challenge of taking on some of the biggest companies in the world were also part of the equation. The Personal Information Protection Commission, or PIPC, was established at a time when South Koreans were becoming increasingly aware of the dangers of their personal information being misused by Big Tech.

Yet, however daunting the task ahead, Yoon was confident about the path the country needed to take to protect individuals' privacy while boosting the use of data by businesses. It was this vision that led him to be chosen to lead the PIPC in the first place.

As for the specific goals, tasks and challenges facing the nascent agency, these involved countless hours of discussions and brainstorming sessions with stakeholders. The PIPC had an urgent priority to develop privacy tools in the Covid-19 pandemic, and an important task to build a blueprint for the agency.

Yet Yoon tells MLex that he feels a sense of accomplishment when looking back over the past 18 months of his agency's operation.

"For me, it was definitely a challenging task, but at the same time, something that could bring a sense of personal achievement," Yoon said, during an hour and a half-conversation in his office in the heart of Seoul's business and cultural district.

BIG TASKS

The first big task that Yoon faced was to build a blueprint for the agency. "We started setting our goals in August 2020 and completed [the list] in November of the same year. Looking at the goals now, I think they came out fine. They're organized in a way that really sets the basis of our agenda," he said.

The PIPC, initially established in 2011, had only served as an advisory body but became an independent data-protection authority in August 2020 with the reform of the Personal Information Protection Act. Creating an independent data-protection authority was also a key requirement to prove South Korea offers an equivalent level of data protection as the EU's General Data Protection Regulation to win an adequacy decision from the EU on cross-border data flows.

Yoon defined the role of the agency as a "control tower" that simultaneously safeguards the protection of personal data and encourages its use by businesses. He said his assignment was particularly challenging because the role of the PIPC is to strike the right balance between the protection of the rights of citizens to their personal data and facilitating the use of data in the digital economy.

The Covid-19 pandemic became the first challenge to that balance. "South Koreans' attitude towards personal data is ambivalent. They admit that the government needed to collect their data to save lives in the pandemic, but concerns were there too as to whether their data was secured and properly protected," said Yoon.

From the beginning of the pandemic, the PIPC took part in devising the contact-tracing scheme with the center for disease control to help manage the data safely and prevent misuse of data by the government. It also came up with ways and tools to prevent excessive data collection, such as eliminating the obligation to leave both names and phone numbers when entering a facility and replacing them with individually assigned random numbers.

ROBUST AGENCY

Yoon envisions the PIPC as a small yet robust organization.

The agency has a staff of 160 and a budget of 50.2 billion won this year, which is about a fifth of the country's communications regulator's yearly budget of 256.1 billion won.

Despite being small in size and budget, the agency has been active in enforcement against companies such as Meta Platform's Facebook and local tech companies, including the controversial AI chatbot developer. From its inception until last year, the agency has announced a total of 324 sanction decisions, imposed 225 corrective orders and imposed fines valued at 16 billion won for violations of the privacy law.

The agency also issued the highest fine of 6.7 billion won on Facebook for illegally sharing data of South Korean users with third-party applications in a probe sparked by the Cambridge Analytica data-privacy scandal in 2018.

The overall evaluation of the new privacy chief is that he is a good moderator who gathers the opinions of the commissioners and facilitates discussions to deliver the best results. Because of the makeup of the commission — three members appointed by an opposition party and two by the ruling party — it is destined to have different opinions with different political views.

The agency's early days were also marked by a particularly challenging case — privacy breaches involving an AI chatbot. The PIPC may be the world's first privacy watchdog to review such a case.

Yoon recalled the AI chatbot case as one of the most difficult cases he and his commissioners encountered. He said it took "a very careful review" and many rounds of discussions with privacy experts and commissioners because the case was unprecedented and there were concerns the agency's sanction decision could somehow work in a way that could hamper future AI technology development.

Yoon has already established a reputation for his effective leadership of the nine-member commission.

The overall evaluation of the new privacy chief is that he is a good moderator who gathers the opinions of the commissioners and facilitates discussions to deliver the best results. Because of the makeup of the commission — three members appointed by an opposition party and two by the ruling party — it is destined to have different opinions with different political views.

MISSION: ERADICATE DATA ABUSE

In the face of soaring privacy breaches, the agency recently added 12 investigators to increase its investigative capabilities.

While coping with privacy concerns from evolving technologies, Yoon has also set himself another priority: to eradicate the misuse of citizens' data by government agencies. He told MLex he was alarmed by the way people's data was handled by government officials in the days before a recent murder. A local district official was found to have leaked the home address of a woman to a stalking suspect, who is alleged to have killed her mother and seriously injured her younger brother after getting their address.

"This should not be considered an individual's fault. We should build a system that could prevent such incidents in the first place," said Yoon.

This led the PIPC to work on measures that could apply to all government agencies to prevent leaks and misuse of personal data by public agencies.

Going forward, he thinks the agency has an important role to play in realizing a user-centric government service platform that runs on Big Data and digital technologies, the so-called "digital platform government" initiative by president-elect Yoon Suk-yeol, who will take office in May.

"Data is the new oil in the digital economy and our role is to safely process data to be made into useful products," said Yoon. "In this respect, the PIPC is a refinery in the digital economy." ■

Why South Korea's privacy-regime overhaul could be a boon for data-using businesses

Businesses in South Korea have been vocal in opposing moves to further update the country's privacy law, warning that the proposed revamp could see a privacy misstep resulting in massive fines — up to a whopping 3 percent of annual global turnover. But the country's top privacy official says there is no cause for panic — and that if anything, the proposed rules could promote companies' active use of data.

It comes as no surprise that South Korea's relatively young data-privacy agency would have plenty of ambitious projects on its anvil. Proliferating digital services, along with the need to safeguard users' privacy from AI and emerging technologies, are all areas of interest for the Personal Information Protection Commission, or PIPC, which was established in 2020.

Meanwhile, the agency also wants to make its mark as the country's lead data-protection authority, with both the power and the willingness to take effective enforcement action in the interest of South Korean businesses and consumers.

Yet the PIPC's mammoth to-do list hinges on lawmakers adopting a second round of amendments to the country's privacy law. Without those changes, the privacy enforcer may be forced to curb its ambition and review its goals. This is why the bill now before parliament is key to the PIPC's future.

The new rules would modernize South Korea's privacy regime with new rights for individuals and measures to make cross-border data transfers more efficient and secure. But most notably for the PIPC, it would award the privacy watchdog the power to impose serious penalties on those caught violating South Korea's privacy law.

For global tech giants, the proposed legislative revamp is provoking real fear. Tech companies are now facing the prospect that a privacy misstep will result in a fine of a whopping 3 percent of annual global turnover — not merely the "relevant turnover," as defined under current rules.

That fear may explain why PIPC chief Yoon Jong-in used a recent interview with MLex to reassure the digital industry and hammer home the message that the proposed revamp offers no reason for panic. Instead, Yoon said he was confident that the changes would promote the active use of data.

SEISMIC CHANGES

In 2020, South Korea's data privacy landscape underwent a seismic transformation, when lawmakers adopted sweeping changes to the country's regime.

The change integrated privacy-related rules extracted from various laws into the Personal Information and Protection Act, or PIPA, which became the primary privacy statute, cutting across both public and private sectors, as well as both offline and online businesses.

Talks over yet another revamp began almost

immediately, however, with the establishment of the PIPC as a central administrative agency responsible for enforcing the law adding to the urgency of further changes.

None of this was surprising: it has always been understood that the privacy overhaul would be done in two phases, with the second round intended to fill any gaps left by the first.

A legislative proposal was swiftly drawn up by the new agency and put out for public comment in January last year. Some eight months later, it was approved by the state council, South Korea's highest executive body, and made its way into the National Assembly for review.

Although the legislation was introduced to the relevant sub-committee late last year, the discussion is now being held up by the shifting political climate following South Korea' presidential election in March, in which a conservative party was elected.

But Yoon believes the process is still on track. "We are actively responding to the Assembly in order to get the bill passed by the end of this year," he told MLex.

INADEQUATE RULES

Yoon sees getting the proposal through parliament as vital, as he tries to strike the right balance between safeguarding the privacy of individuals and encouraging the use of data by businesses — a task he has been entrusted with since his first day as the country's top privacy official.

But the chairman also says that there are now many issues on the front burner. Among these are problems arising from large digital platforms, including Google and Meta Platforms, collecting massive amounts of personal data for their online services; privacy risks associated with emerging technologies including artificial intelligence, facial recognition and the metaverse; and challenges surrounding cross-border data transfers.

But the 11-year-old privacy law, Yoon said, has become central to all considerations because it is inadequate to address all of these concerns that underpin the digital economy.

"The [recent amendment] proposal put forward new privacy rights of individuals — for example, the right to request transmission of their personal information to data controllers and the right to refuse, raise an objection to or request explanation on automated decision making," he said.

The proposed changes would also cover diversified »»

methods for overseas data transfers, which are now only possible with the permission of every individual whose information is being shared, he told MLex.

They would also establish operational regulations for mobile visual-data processing devices, such as drones and autonomous vehicles, he said.

INDUSTRY PUSHBACK

But for the PIPC, there's more at stake than simply getting the policy settings right. Since its inception, the privacy-enforcement agency has been flexing its muscle, lashing out at several tech giants, only to have its powers called into question.

The reason for the pushback against the agency is the size of the fines it has been able to impose — the largest of which was 6.7 billion won (about $6 million) against Meta's Facebook over the illegal sharing of users' data with third-party apps without consent.

Many argued the penalties — capped at 3 percent of sales turnover that is narrowly related to the privacy violation — were too small to act as a deterrent. One lawmaker pointed out that in the US, Facebook was hit by a $5 billion fine, a size unthinkable for the PIPC under existing rules.

If the legislation now before the South Korea parliament were to pass, the PIPC would finally have the powers to impose fines of as much as 3 percent of the "total annual turnover" for non-compliance with the privacy law — the new definition amounting to a substantial enforcement step up for the PIPC.

For the PIPC, there's more at stake than simply getting the policy settings right. Since its inception, the privacy-enforcement agency has been flexing its muscle, lashing out at several tech giants, only to have its powers called into question.

But the proposed change has stirred strong pushback from businesses, which claim the hike is excessive and breaches the principle of administrative fines, which are designed to recover the monetary benefits obtained unfairly through violations.

"It is true that [the greater the maximum fine level], the more companies must work to gain the PIPC's favor," said Kim Young-hoon, head of public policy at Amazon Web Service Korea, during a discussion forum in December.

INVESTING IN PRIVACY

But in his interview with MLex, Yoon stressed that the rise in the fine cap shouldn't be a cause for panic on the part of business. In fact, the move away from criminal punishments to economic penalties should be welcomed.

The hike, Yoon says, would make sanctions more reasonable and effective. Under current arrangements, individuals could face criminal liability for data breaches, with even minor violations leading to possible jail time.

Yoon also noted that, in the revision bill, it has been stipulated that penalties be proportional to the severity of the offense and, as a result, they wouldn't be overly harsh.

"A new rule is also being considered that would exempt companies from paying fines if they faithfully implemented safety measures to secure their customers' personal information," he added.

So, if anything, the legislative change will likely encourage companies to actively do businesses within the legal parameters on the proposed law, Yoon said.

"It is critical for businesses to view privacy as an investment rather than a cost, and I believe that doing so is the only way for firms to secure consumer trust, which is the foundation of success in the digital economy," Yoon said. ■

South Korean privacy chief envisions a two-pronged approach to fixing Big Tech privacy woes

Digital platforms are extracting an unprecedented amount of data from people and businesses that depend on them. This not only poses an enormous risk in the event of a breach, but also gives platforms substantial influence over the everyday lives of millions of people. As regulators in Europe, the US and Asia scramble to regain control of data with new curbs and stronger laws, South Korea's privacy chief is opting for a more nuanced approach that would see a blend of co-regulation and laws to address privacy concerns.

Big Tech and the digital economy. These are the buzzwords on the lips of regulators today, as they grapple with the challenge of reining in the biggest tech platforms such as Google and Meta Platforms.

There are abundant reasons why regulators want to keep the companies in check. They wield tremendous power and can exploit it to charge exorbitant fees, impose restrictive contract terms and engage in other monopolistic practices.

But the major threat capturing increasing attention is that digital platforms extract an unprecedented amount of data from the people and businesses that depend on them — ranging from names and addresses to their habits, preferences and the purchases they make. This massive trove of personal data, often in the hands of a few, powerful operators, not only poses an enormous risk in the event of a breach, but also gives platforms substantial influence over the everyday lives of millions of people.

Many regulators across Europe, the US and Asia are now scrambling to restrict Big Tech platforms with new curbs and stronger regulatory mandates, but Yoon Jong-in, who is committed to both safeguarding and encouraging the use of personal data as South Korea's privacy chief, has a slightly different idea.

In a recent sit-down interview with MLex, Yoon, chairman of the Personal Information Protection Commission, or PIPC, said he sees "enhanced self-regulation" as an answer to at least some of the privacy challenges surrounding Big Tech. Their monopolistic control of data, on the other hand, needs to be broken by new rights and the ability of individuals to move data across platforms, he added.

"I think the best way to approach [these problems] is for the government and companies to share their concerns and work together to come up with rules that both sides can abide by," he said. "The purpose is not to sanction these companies, but rather to protect the privacy of individuals and ensure the safe use of data by making them more accountable."

TRANSPARENCY

Yoon said it is important to understand that at the heart of the platforms' lucrative business model is personal data, which they use to build profiles for targeted advertising, to make product or content recommendations, or to sell the data.

That creates, he said, a responsibility from the »»

platforms to the people they harvest data from — to get informed consent for using the data, to be transparent about the data they collect and what they do with it, and to protect users from harm.

"I get that trade secrets make it difficult for businesses to be transparent, but they need to be as transparent as possible," Yoon said. "Transparency is critical to gaining public trust, which ultimately determines their success."

As a way to elicit greater transparency from large platforms, Yoon proposes what he calls enhanced self-regulation, or co-regulation, in which companies, under the government's guidance, devise rules for safeguarding personal data. This means that although the PIPC lays down the requirements, there is scope to work together to develop security measures that reflect specific conditions and circumstances of each sector.

"Self-regulation didn't really work well because it led to almost no regulation at all," Yoon said. "And this is far better than waiting for something to happen and then slamming companies with sanctions ... The perk is that you get to learn things about a certain market that companies wouldn't have informed you about otherwise."

TESTING THE WATERS

The privacy enforcer has already put the strategy to the test. In November last year, the PIPC and 10 e-commerce giants in South Korea including Coupang, Naver, Kakao and Ebay Korea, kicked off the process of developing a co-regulation plan that, when finished, would govern how the companies, as well as vendors using their services, should process and secure personal data.

The draft plan, which is under revision, contains rules for personal-data access control, access history, encryption and deletion, as well as measures for an added layer of protection such as two-factor authentication, breach detection and blocking tools, and vulnerability checks, according to the PIPC.

The regulator said that once the rules are finalized and in force, the Korea Online Privacy Association will monitor how platforms implement them and the Korea Internet & Security Agency will give technical help as changes arise. The PIPC then plans to revise a relevant administrative-rules notice to reflect the final plan and expand its efforts to develop co-regulation plans with other platforms in the areas of delivery, real-estate, accommodation, mobility and job hunting.

A THREAT TO DEMOCRACY

While co-regulation with platforms can help to reduce the risk of privacy breaches, Yoon believes regulatory interventions by the government will be needed for the biggest challenge — Big Tech's control over users' data.

"Monopolizing data makes them monopolize the market," Yoon said.

The tremendous amount of information tech giants have about users' online activities, such as which websites they visit and what purchases they make, allows them to easily trace individual customers' preferences, which then can be used by companies for customized advertisements and other purposes.

"As witnessed in the Cambridge Analytica privacy scandal, this has the potential for exploitation and manipulation, which could pose a threat to our democracy," Yoon said. "At some point, we will be confused whether my liking of a certain product is out of my free will, or an outcome of being over-exposed to certain product information through targeted advertising."

Big Tech's tracking of online behavioral data is at the core of an inquiry by the PIPC's online platform taskforce, which is devoted to analyzing and examining South Korea's digital advertising markets. The taskforce was formed in February in response to the growing demand from legislators and the media to address issues emanating from the sector.

"Personal information that we are familiar with, such as names and addresses, are no longer a large component of personal data," Yoon said. "When we talk about personal information these days, we're talking about behavioral data collected by tech companies and passed on to [third parties]."

The PIPC's inquiry targets major global tech behemoths such as Google and Meta as well as local tech heavyweights Naver and Kakao, among others. The inquiry is examining whether they are properly collecting the data with users' consent and are in compliance with rules for processing and managing personal information.

"We are still studying the industry to identify the problems and define our position on them," Yoon said. "We are almost halfway through. Each company's policy is different so we're pursuing this on a case-by-case basis."

After completing the probe, the PIPC plans to present a new set of guidelines for the ad tech industry for the practice of offering customized advertising. »»

FIXES FOR BIG TECH DATA MONOPOLY

Yoon said a solution to loosening tech giants' strong grip over data could be to make them share data with smaller competitors.

Instead of letting them treat users' data as their own property and monetize the value of data, users should exercise their right to personal information and share the value that the data brings, he said.

"Personal data holds social, political, and economic value, and it's not right that a few tech companies reap the benefits that data brings," Yoon said.

He believes the MyData services, launched in January, is a first step in this direction. The services, backed by the government, enable South Koreans to move their financial data from one service to another, among some 30 major financial companies, ranging from local banks such as KB Kookmin, Shinhan to BC Card and fintech services Bank Salad and Toss. Through the services, South Koreans can bring together different financial data such as bank records, credit card purchase records, insurance payments and loan repayment records into one major service, and they will have the freedom to make future switches to other services.

The PIPC hopes to apply this data-sharing model across all sectors. It's currently spearheading efforts to standardize data to enable seamless data transfers, so-called data interoperability, across different sectors. It recently hosted the first meeting to embark on the data standardization project with the finance regulator and the education, science and ICT, and health ministries.

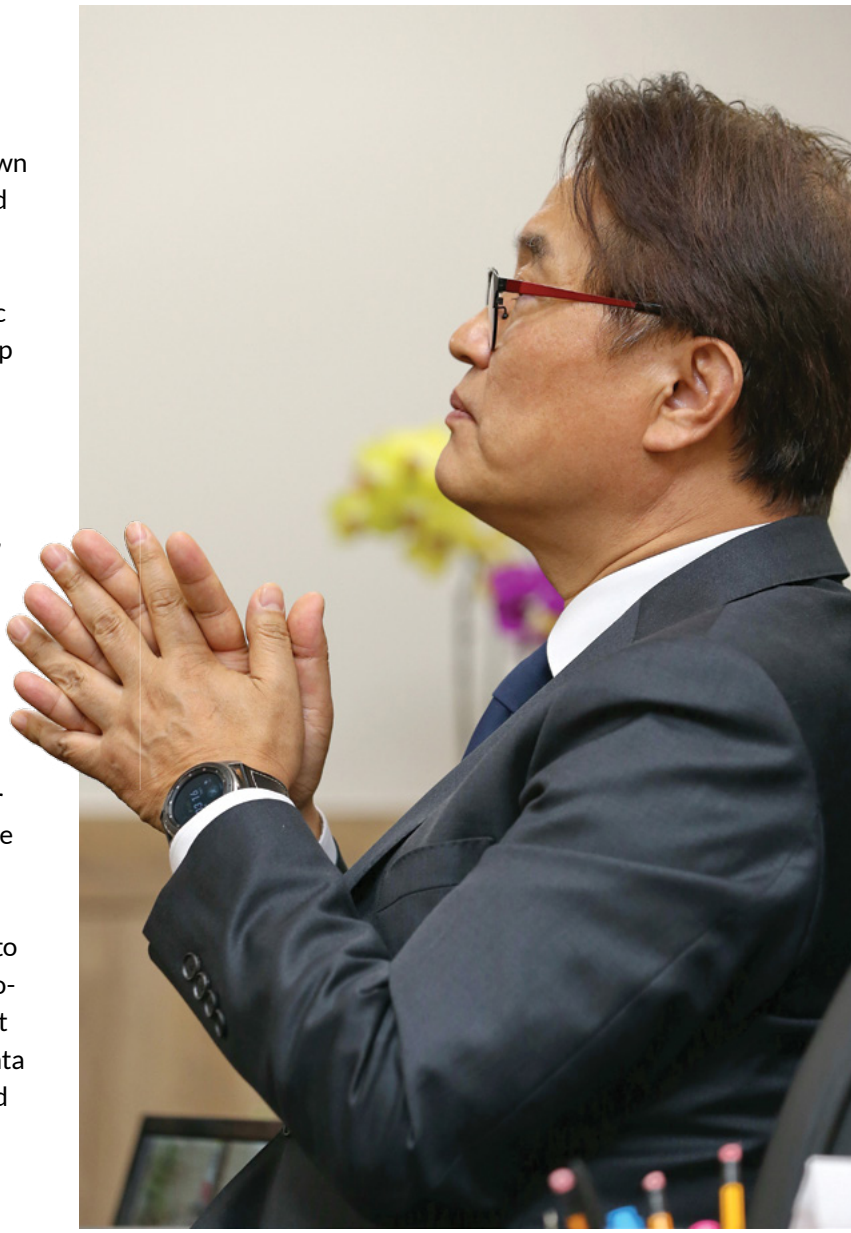
Another solution Yoon is considering is to screen mergers that raise concern for data monopolization.

He has suggested that the PIPC take part in merger reviews by the competition regulator to assess potential anticompetitive effects that data combinations can cause in mergers involving tech companies.

The recent acquisition of eBay Korea by South Korea's retail giant Shinsegae's affiliate E-mart is an example of such a tie-up aimed at maximizing the value of data held by the two online retail giants, Yoon said.

The deal won unconditional clearance from the competition regulator, which determined that the deal poses no risk of substantially limiting competition in the online and offline shopping markets.

"A deal like this requires a more thorough review of data combination," Yoon said. "It requires more than an antitrust perspective." ■



'I get that trade secrets make it difficult for businesses to be transparent, but they need to be as transparent as possible ... Transparency is critical to gaining public trust, which ultimately determines their success.'

Privacy-enhancing technologies key to mitigating risks of personal-data breaches, Yoon says

New privacy-enhancing technologies have been high on the priority list of South Korea's privacy chief since he took on the role in 2020. His agency has already shifted into high gear, unveiling late last year its plan to develop 11 major technologies and dozens of auxiliary ones by 2026 — all with an eye to safeguarding privacy rights of individuals, cutting down on data leaks and ensuring safe data use. He gave MLex an outline of his goals and how he plans to achieve them.

When Yoon Jong-in looks back to the many data leaks and misuses he has had to deal with since becoming South Korea's privacy chief, he feels a sliver of regret.

In the 18 months since he took up his post, sanctions were handed out by the Personal Information Protection Commission, or PIPC, to a wide range of companies, including global tech heavyweights such as Meta Platform's Facebook, Netflix and Microsoft. But its first-ever decision regarding an artificial intelligence, or AI, developer, in particular, seems to have left Yoon with mixed emotions.

While Scatter Lab's indiscriminate collection and processing of personal data for AI development was untenable, personal-data leakages by the company's chatbot Lee Luda, as well as its homophobic and racist rampages, could have been prevented if a technology that filters out sensitive information had been available.

"After I came here, I became acutely aware of the importance of personal-data protection technologies," Yoon told MLex in an exclusive interview. "They can resolve many of the privacy concerns we have today. But little attention had thus far been paid to their development."

That is why new privacy-enhancing technologies have been high on the PIPC's priority list since its launch as the primary enforcer of data privacy in 2020.

The agency has already shifted into high gear, unveiling late last year its plan to develop 11 major technologies and dozens of auxiliary ones by the year 2026 — all with an eye toward safeguarding privacy rights of individuals, cutting down on data leaks, and ensuring safe data use. The PIPC is taking the initiative very seriously, allocating the bulk of its annual budget to this purpose.

"We want to create protection tools that every citizen can use," Yoon says. "That's the goal."

PERSONAL-DATA ECONOMY

Strengthening South Korea's privacy protections has never been more important than it is right now, Yoon argues, when "data is the economy's new oil," propelling changes and innovations in a wide range of industries.

According to government figures, the South Korean data industry is expanding at a breakneck pace, with a market value of 19 trillion won ($15.4 billion) in 2020, up 14 percent from 16.8 trillion won the previous year.

But, as more businesses turn to data to power »»

cutting-edge technologies in areas such as AI, blockchain, and healthcare, the risk of data breaches inevitably escalates. And what's at stake in the event of a breach, according to the PIPC, is vast amounts of personal data, which could be used for harmful purposes.

This has led to a growing anxiety among South Koreans about the possibility that their data could be exploited by companies or sold on the dark web, as seen by the rise in the number of complaints of data leaks each year. A recent survey indicates that a majority of South Koreans view personal information as important.

In 2021, AI chatbot Lee Luda had South Korea reeling, after it went on a spree of bigotry spewing vile slurs against sexual minorities and the disabled, while spilling personal information such as names, addresses, phone numbers and bank account details of individuals. The chatbot's scurrilous comments stemmed from a database of billions of text conversations that Scatter Lab, the startup behind the project, collected through other apps and fed into the AI system — without explicit consent and with little to no safeguards to ensure the privacy of data subjects.

Despite the circumstances, Yoon says there have been meager efforts to research and develop technology to safeguard personal data.

A PATH TO SAFE PERSONAL-DATA USE

Yoon aspires to change all that. Instead of cleaning up messes left by personal-data mishaps, he wants to prevent them altogether by making sophisticated and effective tools available.

For the next four years, the PIPC will spearhead the development of 11 core privacy-enhancing technologies, selected after extensive consultation with various stakeholders, which would guarantee the privacy rights of individuals, minimize data exposure and facilitate the use of personal data within the confines of the country's privacy regime. It has set aside 3 billion won for the project this year, making it one of the top two recipients of the PIPC's 50.2 billion won annual budget.

Among them is a technology that detects online-service providers and third parties collecting or tracking users' behavioral data — their browsing history, search behavior, online purchases, downloads, and overall activity across platforms — without consent and allows them to opt out if they don't want to be tracked.

Other useful tools in the pipeline include a program that identifies illegal transactions involving personal information, including IDs, on the dark web and promptly deletes or disables relevant postings or web servers, a program that filters out personal data from text, video and audio processed by AI chatbots and speakers and a program that anonymizes or pseudonymizes personal information contained in real-time transaction data.

For the next four years, the PIPC will spearhead the development of 11 core privacy-enhancing technologies, selected after extensive consultation with various stakeholders, which would guarantee the privacy rights of individuals, minimize data exposure and facilitate the use of personal data within the confines of the country's privacy regime.

Information-security technologies available today in South Korea are mostly centered on defending computers, servers, mobile devices, electronic systems, and overall data from cyberthreats, and these tools have limits when it comes to protecting data privacy while it is being processed — such as minimizing data exposure, preventing misuse and respecting the rights of data subjects.

There are fewer than 80 firms offering technical solutions for personal-data protection, according to the regulator, most of which are those that detect and encrypt text documents containing personal information and log access history.

One of the technologies that seems to pique Yoon's interest the most is homomorphic encryption, which enables computation to be conducted directly on encrypted data. He says it is "a powerful tool" that can facilitate the sharing of data without compromising sensitive details. "All of these are possible through public-private partnerships," Yoon told MLex. "We are inviting companies and startups to participate in challenges as part of our initiative to secure the technologies." ■

New mobility, AI to be built into legal framework that safeguards South Korean privacy

The second big transition in personal mobility, marked by battery-powered, self-driving and connected vehicles, will bring a change to perceptions of safety, but it is the legal framework governing the privacy and data challenges of new mobility that is capturing the attention of South Korea's top privacy official. Protecting the vast amounts of data generated by new mobility systems from breaches will be key to car safety, Yoon Jong-in told MLex.

Safety features in modern cars are a product of more than a century of hard-fought battles against automakers. The regulations and legal frameworks that ushered in these standards now face an overhaul as automakers, together with technology companies, race to produce the next generation of cars.

The latest transition in personal mobility, marked by battery-powered, self-driving and connected vehicles, will bring a similar change — a new perception of safety and a new legal framework to deal with unforeseen challenges, said Yoon Jong-in, chairman of the Personal Information Protection Commission.

"The vast amounts of data generated from the new mobility systems present new challenges for privacy and security, posing a need to devise a framework for safeguarding data privacy," Yoon told MLex. He expects privacy issues will start to emerge as cars with Level 4 autonomy start to hit the road and get more prevalent when cars achieve full driving automation at Level 5.

Under the South Korean government's prediction, Level 4 autonomous vehicles will be commercialized in 2027 and Level 5 cars by 2035. "When we arrive at the full automation in Level 5, we should expect a car to also become an electronic device that collects a substantial amount of information about individuals," Yoon said.

A Level 5 vehicle will be collecting data via sensors inside and outside and communicating constantly with other vehicles and road infrastructure, as well as location-tracking satellites, to be able to perform under all conditions without human interaction.

The connected car will also serve as a smart device that will enable drivers to pay for coffee and enjoy entertainment while the vehicle drives on its own. The data generated from these activities would be a ripe target for digital thieves.

Yoon says it will be impossible to track and control all the data and check whether it's being managed at every step, but if the system is designed to be secure at the early product development stage, that could mitigate potential privacy risks: "We can make sure privacy is embedded as a default in the early stage of product design, and that's called privacy by design."

"What the agency can do is to create a certification for digital devices that could verify whether the system is designed and made to be safe," he said. "The privacy law can intervene for manufacturers that don't comply with the privacy by design principles."

This way, individuals don't have to worry whether »»

their privacy is protected, and for its part, the regulator won't have to make too many interventions.

Yoon admits the PIPC is still studying the new sector, and a January trip to Hyundai Motor's Namyang R&D center was part of the effort to learn more and get a head start on identifying the privacy challenges. He met company executives, including the autonomous driving division's executive director, to see the latest technology and discuss ways to protect privacy in the new mobility system. According to the PIPC, discussions included ways to protect drivers' privacy when self-driving cars start running on public roads in South Korean cities. They also agreed automakers should collect and retain only minimum information, delete any unnecessary data and protect data with proper encryption.

Yoon said vehicles using today's Level 3 technologies, which only operate on a highway, don't pose high privacy risks as they operate in limited circumstances and drivers can take back control at any time, but the time for full automation is fast approaching. "At some point, we also need to begin working on an international standard," he said. "And that's not one country's job."

PRIVACY BY DESIGN PRINCIPLE

The development of connected and autonomous vehicles is emerging alongside other technologies such as artificial intelligence and smart cities, and Yoon believes privacy by design principles will also play an important role in safeguarding privacy and security issues in these areas.

His proactive approach when it comes to detecting privacy issues in emerging technologies has led to the creation of several industry guidelines.

Last year, the PIPC devised guidelines for the use of personal information for companies developing technologies using artificial intelligence, biometric information and those establishing a smart-city system. In addition to the privacy guidelines for emerging sectors, the regulator released tailored privacy guidelines for organizations, such as hospitals, social welfare facilities, and private academies. In total, the agency has released 21 guidelines since it was launched in August 2020.

The AI technology privacy guidelines, created after an incident where a local AI chatbot developer inappropriately collected and misused text messages containing users' names, addresses and other personal information, was translated into English and presented to other privacy regulators at a recent meeting for the Asia Pacific Privacy Authorities Forum.

"Regulation for emerging technologies has evolved in a way that could hold manufacturers liable for damages caused by their products. For digital devices collecting data, I think we can begin with a certification system based on the idea of product liability," Yoon said. ■

MLex Insight • Commentary • Analysis

Confidently Navigate and Respond to Regulatory Risk

Stay ahead of key regulatory issues with expert insight, commentary and analysis to ensure you are advising your clients on how to best navigate complex, global enforcement environments. MLex is on the cutting edge of reporting on global regulations, both in effect and proposed. Our exclusive, real-time coverage of probes, enforcement trends, litigation and regulator commentary help ensure you are informed and able to respond immediately to client risks and opportunities.

The MLex Difference

- We have a singular focus on regulatory risk, providing unrivalled expertise across our team of 80+ reporters around the world.
- Through longstanding relationships with regulatory communities we keep you informed of developments ahead of mainstream media.
- We insist on the highest standards of sourcing and accuracy in our editorial process.
- Unbiased and forensic reporting ensures our clients get the information they need.

Our Global Presence

Our journalists cover the world from 14 bureaux in key jurisdictions:
EUROPE: Brussels • London **AMERICAS:** Washington • New York • San Francisco • São Paulo
ASIA-PACIFIC: Hong Kong • Beijing • Shanghai • Seoul • Tokyo • Jakarta • Melbourne • Sydney

mlex
a LexisNexis company

UK +44 800 999 3237
US +1 800 356 6547
EU +32 2 300 8250
HK +852 2965 1424
www.mlexmarketinsight.com
customerservices@mlex.com