Schrems looks to China

by Sam Clark ▪ 8 HOURS AGO ▪ 6 MINUTES READ

Press play to listen to this article

0:00 / 8:10

POLITICOPRO
Cyber Insights

By SAM CLARK

with ELLEN O'REGAN

TODAY'S TOP LINE — SCHREMS TACKLES CHINA: The man responsible for taking down two transatlantic data transfer pacts has turned his attention to China — but still has an eye on the U.S.

Welcome to Cyber Insights, POLITICO's cybersecurity and data protection newsletter, giving you the daily lowdown on hacks, leaks and cybersecurity policy chatter in Europe.

How to reach us: Antoaneta is at @antoanetaroussi and aroussi@politico.eu. Sam is at sclark@politico.eu and @sgclark92. Ellen is at eoregan@politico.eu and @ellenoregan.

Laurens is at @laurenscerulus, lcerulus@politico.eu and on Signal and WhatsApp.

DATA PROTECTION

SCHREMS THE SEQUEL? THE GANG TAKES ON CHINA: Last week Austrian privacy group Noyb launched a six-pronged attack on data transfers between the European Union and China, filing complaints with European data protection authorities against TikTok, AliExpress, SHEIN, Temu, WeChat and Xiaomi.

Chinese companies taking off in EU: Noyb founder Max Schrems (who previously led the charge against illegal EU data transfers to the United States) told Cyber Insights that as the amount of EU citizen data traveling to China has "taken off" in recent years, questions have to be asked about how it is being accessed in a country with "even more extreme surveillance laws than the U.S."

Schrems III or Noyb I? Schrems emphasizes that the complaints around EU-China data transfers are "more of a footnote" to previous cases that took down data transfer agreements between the EU and the U.S.

"It's not remotely as big. If TikTok goes down tomorrow, the European economy will really not care," he said.

Speaking of: TikTok went briefly dark in the U.S. over the weekend in a dispute also rooted in concerns about how China might be accessing user data.

Tables turned: Schrems told Cyber Insights it was interesting to see the U.S. on the other side of the data transfer surveillance argument and taking such an "aggressive" stance. "It used to be that the Americans were saying [Europe] is crazy and dramatic, and asking why we have problems with data going abroad. Now they're on the receiving

and asking why we have problems with data going abroad. Now they're on the receiving end suddenly," he said.

Trump factor: As incoming U.S. President Donald Trump is set to deliver his inauguration speech later today, Schrems highlights that the long-running saga of data transfers between the EU and U.S. is far from buried.

"We've basically relied on a rules-based system, where they're going to be nice because we're nice, and everybody loves each other. Moving forward with the Trump administration that's going to be hard to keep up," he said, noting that the existing data transfer deal could be one of the executive orders on the chopping block once Trump takes office.

"There is very little legal value to it, and it can literally be scrapped in a second by Trump ... If tomorrow we don't have a data transfer deal, that would basically mean you would have to shut down [products like] Microsoft 365 tomorrow. I don't think that's going to happen, but if I wake up tomorrow and it happens, I wouldn't be surprised either," he said.

LEGISLATION

WALLET WARS CONTINUE: The EU may have passed its digital identity regulation, eIDAS, but the fight to shape the legislation is not over. Fifteen civil society organizations today wrote to the European Commission demanding that it make the wallet system more transparent.

Looking inside the wallet: Under the eIDAS law, organizations hoping to access information from people's wallets must say what they plan to do with that information, and what type of information they'll take. For example, an online retailer might want your

name and address — but it probably doesn't need your date of birth.

Those organizations must declare those details via a certificate during the registration process, and once they've done so, they can't ask for more info.

'Loophole': According to the organizations, the Commission has proposed a "loophole" that would allow EU member governments to let companies get away without producing one of those certificates.

Such a loophole would allow companies like Facebook to "circumvent the protections and ask European users for everything," if Ireland — where Facebook parent Meta Platforms has its European headquarters — decided not to insist that companies there produce a certificate, they argued.

The long and short of it: "If these loopholes remain, this would have disastrous consequences," the civil society organizations said.

The current Commission proposal "would invite forum shopping and leave users vulnerable to illegal requests for their sensitive information," Thomas Lohninger, from privacy group epicenter.works, told Cyber Insights.

What's next: The Commission has produced a draft piece of secondary legislation, known as an implementing act. It's finished a public consultation and is now awaiting feedback from EU capitals. A meeting and a vote is expected in February.

CYBER POLICY

CROATIA CYBER CRISIS STRATEGY: Croatia recently agreed on a cyber crisis management program, it said on Friday. The strategy sets out procedures for dealing with crises, allocates responsibilities and aligns its own cyber crisis planning with that of

the EU.

AVOIDING CYBER CONFLICT: Representatives of the Organization for Security and Co-operation in Europe (OSCE) will brief EU cyber attachés on its cybersecurity "confidence-building measures" on Thursday, an OSCE spokesperson told Cyber Insights.

Those confidence-building measures, agreed by all of OSCE's member countries, are meant to "reduce the risks of conflict stemming from the use of information and communication technologies," the spokesperson said. They were agreed in two stages in 2013 and 2016 and the OSCE representatives will brief cyber attachés on their implementation.

Pinch of salt: OSCE has mostly European membership, but Russia is also a member and "played an active part" in writing the measures agreed in 2013, according to a statement appended to the initiative.

U.S. CORNER

TRUMP ON CYBER: Donald Trump will re-take his place as U.S. President later today. The first big tech issue on his plate is the TikTok shutdown (and subsequent reversal), but on pure cyber issues, there are more questions than answers, our U.S. cyber colleague John Sakellariadis writes.

They include: Whether the U.S. will take the fight to China, after the major Salt Typhoon hacks on its telecoms network, the fate of an executive order on cybersecurity unveiled by the Biden administration last week, the possibility of scrapping the Cyber Safety Review Board, and the continuation of the Biden administration's approach of forcing,

rather than asking, private companies to up their cyber defenses.

The Europe angle: Trump's effect on the EU's cyber landscape appears likely to fit more into the bigger picture, rather than specific policy issues. His dislike of NATO and his America First approach means Europe has to fend for itself, including on cyber.

ELSEWHERE ON THE WEB

Europol chief said Big Tech has a 'responsibility' to unlock encrypted messages. The Financial Times

Accidents, not Russian sabotage, were behind undersea cable damage, officials said. The Washington Post