As EU privacy law looms, debate swirls on cybersecurity impact

22 May 2018

Credit: CC0 Public Domain

Days ahead of the implementation of a sweeping European privacy law, debate is swirling on whether the measure will have negative consequences for cybersecurity.

The controversy is about the so-called internet address book or WHOIS directory, which up to now has been a public database identifying the owners of websites and domains.

The database will become largely private under the forthcoming General Data protection Regulation set to take effect May 25, since it contains protected personal information.

US government officials and some cybersecurity professionals fear that without the ability to easily find hackers and other malicious actors through WHOIS, the new rules could lead to a surge in cybercrime, spam and fraud.

Critics say the GDPR could take away an important tool used by law enforcement, security researchers, journalists and others.

The lockdown of the WHOIS directory comes after years of negotiations between EU authorities and ICANN, the nonprofit entity that administers the database and manages the online domain system.

ICANN—the Internet Corporations for Assigned Names and Numbers—approved a temporary plan last week that allows access for "legitimate" purposes, but leaves the interpretation to internet registrars, the companies that sell domains and websites.

Assistant Commerce Secretary David Redl, who head the US government division for internet administration, last week called on the EU to delay enforcement of the GDPR for the WHOIS directory.

"The loss of access to WHOIS information will negatively affect law enforcement of cybercrimes, cybersecurity and intellectual property rights protection activities globally," Redl said.

Rob Joyce, who served as White House cybersecurity coordinator until last month, tweeted in April that "GDPR is going to undercut a key tool for identifying malicious domains on the internet," adding that "cyber criminals are celebrating GDPR."

Negative consequences?

Caleb Barlow, vice president at IBM security, also warned that the privacy law "may well have negative consequences that, ironically, run contrary to its original intent."

Barlow said in a blog post earlier this month that "cybersecurity professionals use (WHOIS) information to quickly stop cyberthreats" and that the GDPR restrictions could delay or prevent security firms from acting on these threats.

James Scott, a senior fellow at the Washington-based Institute for Critical Infrastructure Technology, acknowledged that the GDPR rules "could hinder security researchers and law enforcement."

"The information would likely still be discoverable

with a warrant or possibly at the request of law enforcement, but the added anonymization layers would severely delay" the identification of malicious actors.

Some analysts say the concerns about cybercrime are overblown, and that sophisticated cybercriminals can easily hide their tracks from WHOIS.

Milton Mueller, a Georgia Tech professor and founder of the Internet Governance Project of independent researchers, said the notion of an upsurge in cybercrime stemming from the rule was "totally bogus."

"There's no evidence that most of the world's cybercrime is stopped or mitigated by WHOIS," Mueller told AFP.

"In fact some of the cybercrime is facilitated by WHOIS is because the bad guys can go after that information too."

Mueller said the directory had been "exploited" for years by commercial entities, some of which resell the data, and authoritarian regimes for broad surveillance.

"It's fundamentally a matter of due process," he said.

"We all agree that when law enforcement has a reasonable cause, they can obtain certain documents, but WHOIS allow unfettered access without any due process check."

No delays

Akram Atallah, president of ICANN's global domains division, told AFP the organization had tried unsuccessfully to get an enforcement delay from the EU for the WHOIS directory to work out rules for access.

The temporary rule will strip out any personal information from WHOIS directory but allow access to the data for "legitimate" purposes, Atallah noted.

"You will need to get permission to see the rest of the data," he said.

That means the registrars, which include companies that sell websites like GoDaddy, will need to determine who gets access or face hefty fines from the EU.

ICANN is working on a process of "accreditation" to grant access, but was unable to predict how long it would take to get a consensus among the government and private stakeholders in the organization.

Matthew Kahn, a Brookings Institution research assistant, said the firms keeping the data are more likely to deny requests rather than face EU penalties.

"With democracies under siege from online election interference and active-measures campaigns, this is no time to hamper governments' and security researchers' abilities to identify and arrest cyber threats," Kahn said on the Lawfare blog.