The EU's Gift to Cybercriminals

Europe's new privacy rule, called the GDPR, already is thwarting security researchers and police

This article first appeared in *The Wall Street Journal*, May 28, 2018

by Brian E. Finch and Steven P. Farmer

The torrent of news stories about cyberattacks and data breaches never seems to slow, but law-enforcement agencies have tallied some significant victories against online criminals. Websites spewing Islamic State propaganda have been sidelined, thanks to joint efforts by American and European authorities. So have sites on the "dark web" selling illegal drugs, hacking for hire, and other unsavory items and services.

Unfortunately, this good work will now be significantly hindered as the European Union begins to enforce its General Data Protection Regulation. As written, the GDPR will restrict the types of data that companies can share—even, perhaps inadvertently, with law enforcement.

The GDPR is intended to safeguard EU residents' privacy online. To that end, it effectively puts a wide range of "personal data" under cryptographic lock and key. The fundamental problem is that the regulation explicitly covers the kinds of information critical to law enforcement, such as data that could help investigators track down hackers and the devices they use to cause mayhem online.

Take something as basic as the name, physical address and other contact information of the owner for a given website or domain name. Right now those details generally are publicly available in what is called the Whois database, which is maintained by the Internet Corporation for Assigned Names and Numbers, or Icann. Police rely on these kinds of innocuous facts as they work to shut down dangerous websites and find people who host or launch malware.

But the GDPR is being interpreted such that Whois data may not be shared without the owner's consent. As you'd imagine, hackers will decline the opportunity to release data that links them to their crimes. As WSJ Pro Cybersecurity reported May 10: "The problem only surfaced relatively recently as domain name registrars took legal advice about . . . whether sharing the WHOIS data constituted a breach of GDPR. While an exemption would rectify the situation, experts are not confident of a last minute fix."

But unless something is done, police will be robbed of ready access to vital data, drastically impeding their efforts to identify and shut down illicit activity. Icann has proposed allowing law-enforcement officials to regain access to the

Brian E. Finch
Public Policy
+1.202.663.8062
brian.finch@pillsburylaw.com

Steven Farmer
Technology Transactions
+44.20.7847.9526
steven.farmer@pillsburylaw.com

information after they go through a lengthy accreditation program. But even that unwieldy plan is facing objections, including criticism from EU regulators that it would inadequately protect data guarded by the GDPR. As a result, the Whois database is likely to go dark for some time.

Though the GDPR is a product of the European Union, it was deliberately written to cover companies all around the globe. In short, the regulation applies to any business that has a physical presence in the EU or that maintains small morsels of information about EU residents by aiming a website at them or monitoring them. Failure to follow the GDPR's strict data-privacy tenets can invoke eye-watering fines: up to 4% of the company's global revenue or €20 million, whichever is higher.

No government has ever before sought to impose such a sweeping privacy control, perhaps because of the obviously deleterious effects on law enforcement. Already, the GDPR is bearing dangerous fruit. One of the world's leading cybersecurity journalists, Brian Krebs, wrote last month that European-based security companies have become "reluctant to share" internet-address information that could help identify cybercriminals. Previously, security researchers had readily collaborated, but Mr. Krebs worried about a "chilling effect" from the GDPR.

American officials and cybersecurity experts have been raising alarms, with little result. Commerce Secretary Wilbur Ross wrote to EU officials in early April, saying that under the GDPR America's ability to combat cybercrime "could be seriously harmed." He asked for "temporary forbearance from GDPR enforcement on the processing of WHOIS information."

Everyone values privacy. But the regulatory rubric the EU has created will make it harder than ever to catch computer hackers and other online criminals. Governments world-wide should be urgently pressing the EU to change this disastrous aspect of the regulation. Absent serious pressure, real reform will probably still come—but only after America and other nations are hit by a tidal wave of GDPR-enabled cybercrime.