Backdoors that let cops decrypt messages violate human rights, EU court says

Ashley Belanger - 2/14/2024, 4:49 PM ⋮ 5-6 minutes ⋮ 2/14/2024

Alternative means to access encrypted messages

To weigh the case, the ECHR also reviewed reports from the United Nations that found that "encryption is a key enabler of privacy and security online and is essential for safeguarding rights, including the rights to freedom of opinion and expression, freedom of association and peaceful assembly, security, health, and non-discrimination." According to the UN, encryption protects free speech in communities experiencing censorship, shields important work from journalists and human rights defenders, offers security to women fleeing harassment and violence, and is "indispensable" to civilians during armed conflicts.

Efforts by governments to weaken encryption to scan messages for information connected to crimes like sharing child sexual abuse materials (CSAM), human trafficking, or terrorism create a "dilemma" for governments that also want to protect vulnerable populations from mass surveillance and cybercrimes, the UN said.

Careful review confirmed that the government's legitimate interest, the UN reported, is outweighed by society's rights to privacy, as well as freedom of expression that could be chilled if encryption was weakened or if messaging services chose to alter or withdraw encryption in regions requiring disclosures.

Beyond impacting regions passing laws weakening end-to-end encryption, the UN found, "such adverse effects are not necessarily limited to the jurisdiction imposing the restriction; rather it is likely that backdoors, once established in the jurisdiction of one State, will become part of the software used in other parts of the world."

The Council of Europe agreed that backdoors could be problematic, finding that backdoors created for law enforcement "could easily be exploited by terrorists and cyberterrorists or other criminals," potentially exposing messaging services users to more harms than benefits from enabling decryption to aid investigations. Especially considering that "independent reviews carried out in the United States" found that "mass surveillance does not appear to have contributed to the prevention of terrorist attacks, contrary to earlier assertions made by senior intelligence officials," the Council noted.

Rather than require access to encrypted messages, law enforcement agencies have alternatives, the UN said, including "improved, better-resourced traditional policing, undercover operations, metadata analysis, and strengthened international police cooperation." EISI pointed out that officials could also attempt to guess or otherwise obtain private keys of suspects, perhaps by exploiting software vulnerabilities on suspects' devices or seizing devices.

"While indiscriminate backdoors might be cheaper for the State than alternative investigative measures, they were expensive for society at large on account of the security risks they produced," EISI told the ECHR.

Europol and the European Union Agency for Cybersecurity (ENISA) recommended removing regulators' and law enforcement's focus from "breaking the protection mechanism" and putting it back on getting access to communications through typical police tactics.

"Solutions that intentionally weaken technical protection mechanisms to support law enforcement will intrinsically weaken the protection against criminals as well, which makes an easy solution impossible," Europol and ENISA said.

"Weakening encryption by creating backdoors would apparently make it technically possible to perform routine, general, and indiscriminate surveillance of personal electronic communications," the ECHR's ruling said. "Backdoors may also be exploited by criminal networks and would seriously compromise the security of all users' electronic communications. The Court takes note of the dangers of restricting encryption described by many experts in the field."

EISI's Husovec told Ars that ECHR's ruling is "indeed very important," because "it clearly signals to the EU legislature that weakening encryption is a huge problem and that the states must explore alternatives."

If the Court of Justice of the European Union endorses this ruling, which Husovec said is likely, the consequences for the EU's legislation proposing scanning messages to stop illegal content like CSAM from spreading "could be significant," Husovec told Ars.

During negotiations this spring, lawmakers may have to make "major concessions" to ensure the proposed rule isn't invalidated in light of the ECHR ruling, Husovec told Ars.

Previous Chapter Next Chapter