Germany Rushes to Expand Biometric Surveillance

Svea Windwehr ⋮ 5-6 minutes ⋮ 10/7/2024

Germany is a leader in privacy and data protection, with many Germans being particularly sensitive to the processing of their personal data – owing to the country's totalitarian history and the role of surveillance in both Nazi Germany and East Germany.So, it is disappointing that the German government is trying to push through Parliament, at record speed, a "security package" that would increase biometric surveillance at an unprecedented scale. The proposed measures contravene the government's own coalition agreement, and undermine European law and the German constitution.In response to a knife-stabbing in the West-German town of Solingen in late-August, the government has introduced a so-called "security package" consisting of a bouquet of measures to tighten asylum rules and introduce new powers for law enforcement authorities.Among them, three stand out due to their possibly disastrous effect on fundamental rights online.

Biometric Surveillance

The German government wants to allow law enforcement authorities to identify suspects by comparing their biometric data (audio, video, and image data) to all data publicly available on the internet. Beyond the host of harms related to facial recognition software, this would mean that any photos or videos uploaded to the internet would become part of the government's surveillance infrastructure.This would include especially sensitive material, such as pictures taken at political protests or other contexts directly connected to the exercise of fundamental rights. This could be abused to track individuals and create nuanced profiles of their everyday activities. Experts have highlighted the many unanswered technical questions in the government's draft bill. The proposal contradicts the government's own coalition agreement, which commits to preventing biometric surveillance in Germany.The proposal also contravenes the recently adopted European AI Act, which bans the use of AI systems that create or expand facial recognition databases. While the AI Act includes exceptions for national security, Member States may ban biometric remote identification systems at the national level. Given the coalition agreement, German civil society groups have been hoping for such a prohibition, rather than the introduction of new powers.These sweeping new powers would be granted not just to law enforcement authorities--the Federal Office for Migration and Asylum would be allowed to identify asylum seekers that do not carry IDs by comparing their biometric data to "internet data." Beyond the obvious disproportionality of such powers, it is well documented that facial recognition software is rife with racial biases, performing significantly worse on images of people of color. The draft law does not include any meaningful measures to protect against discriminatory outcomes, nor does it acknowledge the limitations of facial recognition.

Predictive Policing

Germany also wants to introduce AI-enabled mining of any data held by law enforcement authorities, which is often used for predictive policing. This would include data from anyone who ever filed a complaint, served as a witness, or ended up in a police database for being a victim of a crime. Beyond this obvious overreach, data mining for predictive policing threatens fundamental rights like the right to privacy and has been shown to exacerbate racial discrimination.The severe negative impacts of data mining by law enforcement authorities have been confirmed by Germany's highest court, which ruled that the Palantir-enabled practices by two German states are unconstitutional. Regardless, the draft bill seeks to introduce similar powers across the country.

Police Access to More User Data

The government wants to exploit an already-controversial provision of the recently adopted Digital Services Act (DSA). The law, which regulates online platforms in the European Union, has been criticized for requiring providers to proactively share user data with law enforcement authorities in potential cases of violent crime. Due to its unclear definition, the provision risks undermining the freedom of expression online as providers might be pressured to share rather more than less data to avoid DSA fines.Frustrated by the low volume of cases forwarded by providers, the German government now suggests expanding the DSA to include specific criminal offences for which companies must share user data. While it is unrealistic to update European regulations as complex as the DSA so shortly after its adoption, this proposal shows that protecting fundamental rights online is not a priority for this government.

Next Steps

Meanwhile, thousands have protested the security package in Berlin. Moreover, experts at the parliament's hearing and German civil society groups are sending a clear signal: the government's plans undermine fundamental rights, violate European law, and walk back the coalition parties' own promises. EFF stands with the opponents of these proposals. We must defend fundamental rights more decidedly than ever.