#tiktokcringe: Targeted Ads Are No 'Legitimate Basis' for Data Processing, Says Italy's Data Privacy Protection Authority

Published by *Kattison Avenue* | Issue 9

September 28, 2022

European data authorities are increasingly united in policing data and privacy violations

By Cynthia Martens

It began, innocently enough, with an update to TikTok's privacy policy. Via upbeat messaging, users learned that they would soon receive "personalized" advertising based on their activities on the trendy video platform, now the world's most downloaded app for those aged 18 to 24, who even use it as a search engine.

But on July 7, Italy's data privacy protection authority, the Garante per la Protezione dei Dati Personali (Garante), issued a sharply-worded ruling against Tik Tok, warning that using personal data automatically archived on users' devices to send them targeted ads is illegal without the users' explicit consent.

American companies, take note: alongside its counterparts in other European Union member states, the Italian Garante is a powerful legal entity, a collegiate body withdepartmental branches dedicated to fields such as health, human resources, marketing, freedom of expression and cyberbullying, among many.

"Its investigative powers are quasi absolute. It is even above state secrets. But, at the same time, its inspection and enforcement activities are limited to the realm of personal data violations. That always has to be the spark that lights the fuse," said Pierluigi Perri, an Italian lawyer and professor at the University of Milan with expertise in data protection and web surveillance.

Outside the TikTok ruling, the Garante has drafted guidelines on the use of cookies and other tracking tools; penned ageneral application order concerning biometrics; issued a general injunction regarding "silent calls," or unsolicited telephone calls in which individuals answer their phones but are not put through to any speaker; and commented on the legality of vehicle geo-location in the context of employer-employee relations.

Headquartered in Rome, the Garante has an advisory function, working with the Italian Parliament to ensure new laws comply with data protection legislation and making recommendations to various executive branches of government. It also has the authority to impose administrative sanctions and accessory sanctions, which could include an order to stop processing data — a move that would send shivers down the spines of social media executives. On the other hand, the Garante cannot issue criminal sanctions; it can only refer crimes to the prosecutor's office. And it cannot order the payment of damages. Individuals seeking redress for data privacy violations may go to court or to the Garante, but they cannot do both.

The ability of advertisers to purchase web data andtarget individual consumers has been of special concern to lawmakers, and Europe has been ahead of the curve on privacy legislation,much to the chagrin of Silicon Valley. Since the European Union adopted the General Data Protection Regulation (GDPR) in 2016, the European Data Protection Board (EDPB) has worked to ensure its consistent application throughout the European Union.

TikTok had cited "legitimate interest" under the GDPR as the legal basis for its data processing and advertising practices. The facts, however, suggested to the Garante "that TikTok's choice is merely instrumental to achieving its own goals, whereas the legitimate basis for data collection appears to be of secondary importance, adaptable to the circumstances," as stated in the ruling.

Pasquale Stanzione, president of the Garante, law professor and one of Italy's leading authorities on privacy and consumer protection, authored the TikTok opinion. In an interview for Kattison Avenue, he acknowledged that "using 'legitimate interest' as a lawful premise for data processing requires an undoubtedly complex, fact-specific analysis." In addition to reiterating that consent was the only appropriate basis for TikTok's proposed processing of personal data for targeted advertising, he expressed concerns over the platform's attractiveness to minors, noting that the limits of current age verification tools mean that targeted advertising "could reach the youngest users, including with inappropriate content."

Exactly what a "legitimate basis" is in this context continues to ruffle feathers in Europe. Article 6 of the GDPR allows for the processing of personal data only if and to the extent that at least one of six conditions applies, including the catch-all that processing is necessary "for the purposes of the *legitimate interests* pursued by the controller or by a third party, except where such interests are

overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

"Legitimate interest is what I tell my students is the unicorn of privacy because it's hard to understand exactly what it is," Prof. Perri said during an interview for *Kattison Avenue*. "It's a legal doctrine that allows one party to process the other's data on the basis of mutual interest. So, we're both benefiting without saying anything — there is no contract, no need for anything formal and the data processing can go ahead without explicit consent." He cited prevention of fraud or a pre-existing commercial relationship between the parties as textbook examples.

From a commercial advertising perspective, of course, consent is less valuable than legitimate interest because internet users can withdraw their consent at any time. As one *Harvard Business Review* writer noted, "One of the biggest pain points in the era of consent is the potential loss of data."

According to Eurostat, the statistical office of the European Union, in the decade between 2011 and 2021, the share of European households with internet access rose from 72 percent to 92 percent, with highest access levels reported in urban areas. One of the most common online activities in Europe in 2021 was social networking. Eurostat also reported that 53 percent of all European internet users had refused to allow the use of their personal information for advertising, while 39 percent claimed to read privacy policy statements before providing personal information. Awareness of online tracking via cookies was especially high — 86 percent — among European internet users aged 16 to 24.

Prof. Perri said European consumers, broadly speaking, are more concerned about the use of their personal data by corporations than by the government, whereas worries run in the opposite direction in the United States.

In addition, the philosophical framing of data privacy rights has led to different legislative approaches in Europe and the United States. Whereas US laws frequently anchor privacy to personal choice, he said European law centers on "protecting personal dignity" and a "strong notion of privacy as a fundamental right" found in Articles 8 and 9 of the Charter of Fundamental Rights of the European Union. Because fundamental rights are non-negotiable, European lawmakers tend to view with suspicion the use of personal data for advertising and marketing or even as payment for services.

"The European Union showed extraordinary foresight in its understanding, back in 1996, of the importance of legislation protecting individuals with respect to the increasingly pervasive processing of their personal data," Prof. Stanzione said, noting that the lack of regulation of the internet early on led to a dramatic power imbalance between large corporations and consumers. He described the

GDPR as a "broad, futureproof legal framework" that sought to withstand the inevitable evolution of technology, adding that a robust protection for internet users can only stem from their freely given, specific, unambiguous and informed consent to data processing. "One of the greatest successes of [European] privacy law has been increasing public awareness of the importance of protecting our freedom by protecting our data," he said.

Despite its sweeping authority, from the outset, the Garante has suffered from a lack of resources. "Already my predecessors publicly complained about the lack of funding allocated to the Garante considering its duties, especially when compared to other European authorities and even other Italian authorities," Prof. Stanzione said. While a 2021 legislative degree offered some relief, Stanzione said the entity is in urgent need of greater staffing as privacy and data protection issues proliferate. "Just consider that only a few staffers are assigned to work on telemarketing matters," he noted.

Through a protocol agreement in 2002 that was most recently renewed in 2021, Italy's tax police, the Guardia di Finanza (known as the GdF), has assisted the Garante in carrying out inspections. Prof. Stanzione said the GdF's support has been crucial, given the Garante's limited resources and the fundamental rights it is charged with protecting.

Disparities in member-state resources notwithstanding, advertisers and other data processors should recognize the increasingly powerful cohesiveness of European data authorities. Prof. Stanzione referred to such cooperation as "the defining feature" of European privacy law, despite the fact that it is time-consuming, a challenge given "the short time frames that characterize the relationship dynamics between users and platforms in our digital society."

He expressed confidence in Europe's Digital Services Act package, composed of the Digital Services Act andDigital Markets Act, which is in the final stages of approval after its formal adoption by the European Parliament this summer. With the European Council's stamp of approval, the package will enter into force 20 days after the underlying acts are published in the Official Journal this fall.

"Both of these measures move in the direction of a much-needed adaptation of consumer protection to the unique demands of a constantly evolving digital reality, by providing users with a range of tools to proactively exert broader control over their data," he said. "At the same time, they reinforce the obligations — of disclosure, loyalty, honesty, but, more generally, responsibility — of platforms, aiming to align freedom of expression, freedom of economic initiative and the protection of fair competition, while also shielding users from improper uses of their personal data."

Prof. Perri noted that the EDPB is now discussing parameters for administrative sanctions by member-state data protection authorities to promote greater uniformity. He also said that there has been effective coordination among the entities in issuing sanctions related to use of "cookie

walls," which prevent users from accessing services unless they consent to share their data. The EDPB took a stand against cookie walls in 2020.

TikTok, meanwhile, has hit pause on that privacy policy update.

To read the full newsletter, please click here.