

Top Google Executives Found Criminally Liable For Privacy Violations

Francis M. Buono
Gianluca Cattani
and Sophie Keefer

WILLKIE FARR & GALLAGHER LLP

Google's Chief Legal Officer, Chief Privacy Counsel, and former Chief Financial Officer have each been sentenced to six months in prison by an Italian court for violating the country's privacy laws. The decision (the "Decision"), issued by the Criminal Court of Milan (the "Court") on February 24, 2010, and published on April 12, 2010, is the most recent and most dramatic demonstration of the need for companies doing business in Italy – and in Europe generally – to pay close attention to, and maintain strict compliance with, such countries' privacy laws. The Decision also raises serious questions about whether Internet service providers and Internet content providers that allow third-party content on their services or websites need to increase their screening, monitoring, and/or removal of any such content that might violate local privacy or other laws.

The Claims Against Google

The case stems from an incident in 2006 when students at an Italian school filmed and then uploaded a three-minute video clip to the now-defunct Google Videos site showing high school students bullying a schoolmate with Down syndrome.

An Italian advocacy group for people with Down syndrome and the boy's father reported the existence of this video to the police. Following an investigation, the three Google officers were indicted. Prosecutors' key charge against Google was that it should not have allowed the posting of the video or should at least have become aware of the video sooner and taken it down. The video had been on the Google Videos site for two months, had apparently been viewed over 5,000 times, and at one point was placed on the site's list of "most entertaining" videos. Google argued to the Court that it was impossible for the company to monitor every video posted on its sites, and stressed that the company had removed the offending video within hours of receiving notification from Italian authorities and had cooperated to help identify the bullies and bring them to justice (they were each sentenced to ten months of community service). The prosecutor responded that some users had posted comments earlier asking for the video to be taken down, but that Google did not act.

Privacy-based Decision

The main focus of the 111-page Decision, drafted by Judge Oscar Magi, was that the abused individual's privacy had been violated. European law broadly protects individuals' privacy rights. Specifically, Article 8 of the European Convention on Human Rights provides, "Everyone has the right to respect for his private and family life, his home and his correspondence." In Europe generally, therefore, privacy is a fundamental human right that often is viewed as trumping all conflicting rights, even if that has negative financial ramifications for a defendant.

Francis M. Buono is a Partner in the Communications, Media & Privacy practice at Willkie Farr & Gallagher LLP in the Washington, DC office. Gianluca Cattani is a Partner in the Corporate and Financial Services Department of Delfino e Associati, the Italian affiliate of Willkie Farr & Gallagher LLP in Rome. Sophie Keefer is a Senior Associate in the Communications, Media & Privacy practice at Willkie Farr & Gallagher LLP in the Washington, DC office. Mr. Buono, Mr. Cattani, and Ms. Keefer advise a broad range of clients on domestic and international data privacy and data security issues.

The privacy laws in Italy are particularly strict. Notably, article 167 of Legislative Decree no. 196 dated June 30, 2003 (the "Personal Data Protection Code") provides that any person who, with a view to gain for himself or another or with intent to cause harm to another, processes personal data in breach of certain rules set forth in the Personal Data Protection Code (such as the requirement to obtain the consent of a data subject/owner, and to prepare disclosure documents relating to the scope and purpose of data processing) may be sentenced to jail for up to three years if convicted. As noted, the three Google executives were each sentenced to six months in prison for violating the privacy of the abused individual.

EU legislation and Italian law also provide that Internet service providers ("ISPs") are not responsible for monitoring third-party content on their sites, but must remove such content if they receive complaints; Internet content providers, by contrast, are responsible for the things they "publish." Google had argued that it falls into the former category, but the Italian prosecutor disagreed, responding that the search company is an Internet content provider, rather than an ISP, and was therefore in breach of the same Italian law that regulates newspaper and television publishers.

The Court held that there is no general obligation, even for an Internet content provider, to exercise "preventive control over data entered into the system" or to ensure that personal data processed is collected by third parties in accordance with the Personal Data Protection Code. Rather, despite acknowledging the "more delicate" position of Internet content providers and noting that an "active host" such as Google Italy has greater means of recognizing a crime committed by an individual user, the Court assigned little value to the distinction between ISPs and Internet content providers in its assessment of the obligations placed upon owners or operators of websites by the Personal Data Protection Code. For both categories, said the Court, there exists an obligation to correctly and promptly inform users about the obligations under the Personal Data Protection Code. The Court found that the privacy policy viewable by users on the Google Videos home page, which explained the details of Google's video posting/submission process, was "so hidden in the general terms of use as to render it completely ineffective for the purposes provided for by law." In fact, the Court held that the convictions of the Google executives were not based upon a general obligation of control over data input, but rather the result of an "insufficient . . . statement of legal obligations" with respect to the user privacy policy and related disclosure requirements.

Finally, the Court stated that the Google executives bore responsibility for the privacy violation because Google profited from the video by selling advertising on the site where the footage was posted. Judge Magi wrote in the Decision that it was clear that Google's violation of the privacy law was based on its desire for financial gain: "The service was deliberately launched without monitoring and only later – given its enormous success – was the possibility introduced for users to report inappropriate content for the purpose of its removal . . . [And the] technical and personnel investments [for responding to such user reporting] were ridiculously inadequate for the purpose." Judge Magi concluded, "In simple words, it is not the writing on the wall that constitutes a crime for the owner of the wall, but its commercial exploitation in certain cases and circumstances can constitute a crime."

The Google executives will not serve prison time because of Italian criminal law rules on suspension and commutation of short prison sentences for first-time offenders.

Nonetheless, Google has confirmed that it will vigorously appeal the Decision.

Comparison With U.S. Law

U.S. laws protect privacy as well, but to a different degree than do the laws in Europe. Whereas U.S. privacy laws generally are designed to protect consumers against abuses by businesses or against government intrusions, EU privacy laws focus more broadly and more fundamentally on protecting people from having their lives exposed to public view, especially in the mass media. As the prosecutor in this case summarized Italian law, "A company's rights cannot prevail over a person's dignity." Although the U.S. also recognizes a tort for invasion of privacy when one appropriates for his own use or benefit the name or likeness of another without the other's consent, this right may be outweighed by stronger interests and protections in the U.S. under First Amendment principles and jurisprudence.

For example, under the U.S. Communications Decency Act of 1996 (the "CDA"), "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." The CDA generally has been interpreted by U.S. courts to extend broad immunity for online service providers from defamation and/or other potential liability. Starting with *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997), cert. denied, 524 U.S. 937 (1998), U.S. courts have generally been reluctant to impose a duty on online service providers to monitor the third-party content posted to their websites, or to hold them liable as a result of such postings. In *Joyner v. Lazzareschi*, No. 05-10627 (Cal. Ct. App. March 18, 2009), for example, a California court held that an online service provider was immune from liability under the CDA in connection with communications in an online forum, even though the provider republished the allegedly defamatory comments on a different website.

To be sure, some cases – such as *Fair Housing Council v. Roommates.com*, 521 F.3d 1157 (9th Cir. 2008) (holding that a website's provision of a questionnaire inviting users to indicate an unlawful roommate preference, i.e., preferred sexual orientation, made the website legally liable under the Fair Housing Act for the resulting user inputs) – have started to question the extent of this immunity. However, in general the attitude and resulting law in the U.S. is to afford online service providers broad protection from liability.

Similarly, the Digital Millennium Copyright Act of 1998 (the "DMCA") provides immunity for online service providers from copyright liability based on the content of third-party postings to their sites, so long as the provider complies with the DMCA's steps regarding proper notice and take-down of potentially infringing content once the provider becomes aware of it.

Given this more flexible approach to striking the balance between individual privacy and online freedoms, it is no surprise that the U.S. is usually the venue where new online enterprises based on user-generated content (e.g., eBay, YouTube, Facebook) are created. However, since the Internet is a global phenomenon, the Decision must be taken seriously by multinational organizations doing business in Italy and in other countries with similarly restrictive privacy laws.

Key Implications/Recommendations

Although Judge Magi's opinion dismissed as "much ado about nothing" criticism that the Decision will negatively impact the Internet, many view the Decision as having potentially significant implications and posing new risks for online service providers doing business in Italy and beyond. A Google spokesperson commented, "We don't see any silver lining to the decision. We believe it is

an extremely dangerous decision." U.S. ambassador to Italy David Thorne said that the U.S. was "disappointed" by the ruling, which he described as a blow to the freedom of the Internet.

In the wake of the Decision, it has been reported that German and Swiss privacy regulators have initiated investigations into whether the practice of posting photos, videos, and other information about people on sites such as Facebook, without their consent, is a breach of privacy laws.¹

Companies subject to the Decision should undertake the following:

Enhance the Process to Remove Objectionable Online Content. Online service providers that accept the posting of third-party content must be aware that they could be held liable for that content in Italy and perhaps in other countries as well, particularly if they are profiting from the service through subscription or advertising fees. Such companies should review and, if necessary, enhance the screening process they use to allow the posting of such content and should be prepared to respond quickly when complaints about allegedly offensive or illegal third-party content arise, even if such complaints come from other users instead of government authorities. In this sense, it is worth noting that Google's YouTube service now employs a more comprehensive sign-up process before a user is allowed to upload videos and has made it easier for users of its platform to identify and report on videos that may be problematic for legal reasons or reasons of taste.

Enhance Online User Notices. Online service providers should also review their online privacy policies and terms of use to ensure that the details of how users may post content are complete and not "hidden" among other general contractual terms of use, and that such policies clearly inform users about their obligations to respect and protect individuals' privacy under applicable laws such as Italy's Personal Data Protection Code. In this exercise, companies should bear in mind that pictures, photos, and videos are considered personal data under the laws in Italy and other EU countries.

Review General Privacy Compliance. Finally, this case should serve as a wake-up call for all companies – doing business both online and offline – about the stricter privacy laws that exist, and that are aggressively being enforced, in Europe. As noted above, Europeans consider privacy a fundamental human right that often trumps other competing interests, including freedom of speech and any significant financial burdens required to achieve compliance. Many of these laws, including the EU's Data Protection Directive adopted in 1995 and the various laws in the 27 EU Member States, carry with them the possibility of criminal penalties for violations. As such, companies doing business abroad should take this opportunity to ensure that they have filed any required privacy registrations with foreign Data Protection Authorities regarding their processing of personal data, and that they are otherwise in compliance with the stricter EU-style privacy laws, which, if not respected, could have dramatically negative impacts on their business.

* * *

Multinational corporations would be well advised to take the foregoing steps rather than being lulled into a false sense of security by relying on the currently more flexible and business-friendly legal regime in the U.S., only to find, as Google unfortunately did, that stringent privacy laws in certain other countries can pose significant risks and result in significant penalties for them and their employees.

¹ See Frank Jordans, "Privacy Regulators Taking Aim at Your Online Photos/Vids," *The Associated Press*, March 24, 2010.