



# ITALIAN APPEALS COURT OVERTURNS GOOGLE PRIVACY CONVICTIONS

The appellate court in Milan recently published its decision overturning the conviction of three Google executives on charges of Unlawful Data Processing in violation of Article 167 of the Italian Privacy Code. The executives—who were high-level business and legal officers—were given suspended six-month prison sentences by a Milan assize court in February 2010 for allowing video depicting the bullying of an autistic teenager to be uploaded to the Italian Google Video web site, which was the precursor to Google Italia YouTube. The appellate court’s decision serves as a significant precedent with regard to intermediary liability, data protection and privacy law, and corporate responsibility.

## BACKGROUND

Under European Union law, hosting providers are not liable for the content they host, as long as they promptly comply with official takedown orders or otherwise appropriately respond when receiving notice of improper content (see Art. 15 of Directive 2000/31).

Nevertheless, the public prosecutor sought to hold the Google executives, none of whom were based in Italy, criminally liable for privacy violations due to Google’s failure to exert a preemptive screening of the video prior to hosting it on the Google Video web site.

In convicting the executives, the assize court found the executives culpable for Google’s failure to inform providers of content of Italian privacy requirements and the ramifications of violating data protection pursuant to Article 13 of the Italian Privacy Code. Google’s position in the lower court, and on appeal, was that as an internet service provider, it could not be held liable for the content of the media its users upload to the internet.

## APPELLATE RULING

In overturning the convictions, the appeals court limited the application of intermediary liability to internet providers that merely host user-generated

content. The court rejected the public prosecutor's position that hosting services must preemptively screen all material uploaded to the internet, explaining that such a duty could chill freedom of expression. As the court stated:

Imposing a duty on or granting the power to, an Internet provider to carry out prior screening seems to be a step that is to be afforded particularly careful consideration, given that it is not entirely free of risk due to the possibility of a conflict arising with the principles of freedom of expression of thought.

The court held that internet platforms, like Google Video or YouTube, are not responsible for user-uploaded content, absent notice of inappropriate content. The court found that "the possibility must be ruled out that a service provider, which offers active hosting can carry out effective, preemptive checks of the entire content uploaded by its users." Such an obligation would impose a "pre-emptive filter on all the data uploaded on the network, which would alter [the network's] functionality."

The court further explained that "it is patently clear that any assessment of the purpose of an image contained in a video, capable of ascertaining whether or not a piece of data is sensitive, implies a semantic, variable judgment which can certainly not be delegated to an IT process."

The court's opinion, therefore, establishes that users who upload content to the internet are responsible for compliance with data privacy laws, as automated processes are ill-equipped to review content for privacy concerns. By placing accountability on the users who upload content, rather than the hosting site, the appellate ruling parallels case law from the European Court of Justice and the European Parliament's report on the legal liability of internet service providers (see Corte d'Appello di Milano, case 4889/2010, pg. 21).

Finally, the court recognized that employees of internet providers cannot harbor the requisite *mens rea* to violate data privacy laws where they lack direct knowledge of the offensive content or data privacy violation.

## SIGNIFICANCE

In overturning the convictions, and rejecting the public prosecutor's argument, the appellate court's opinion reduces the potential burdens facing content hosting providers and other similar internet companies. Had the public prosecutor prevailed, it would have required internet companies and their executives to ensure that hosted content did not violate the rights of those depicted, mentioned, or otherwise implicated by user-uploaded media. Prescreening all user-uploaded content would have been both cost-prohibitive and unwieldy for internet hosting services providers, both large and small.

Rather than require prescreening of the voluminous data uploaded on a daily basis, the ruling requires the companies to act once they receive notice of content that implicates privacy concerns. This seems to be consistent with European Union regulations, which require member states to ensure that hosting providers not be held liable for user-generated data absent notice of illegal activity (see Art. 14 of Directive 2000/31), and that no general obligations be placed upon hosting sites to continuously monitor user-generated data to ensure a lack of illegal activity (see Art 15 of Directive 2000/31).

Nevertheless, the criminal prosecution of the executives serves as a reminder of the increasing importance governments are placing on consumer privacy and the concomitant necessity for effective and efficient notice and takedown regimes. Companies with web sites offering the possibility for user-generated content should continuously review their programs and processes for receiving and reviewing reports of inappropriate or otherwise unlawful content hosted on their servers, and ensure that the proper mechanisms are in place to rapidly address complaints upon notice.

## LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at [www.jonesday.com](http://www.jonesday.com).

### **Katherine S. Ritchey**

San Francisco

+1.415.875.5728

[ksritche@jonesday.com](mailto:ksritche@jonesday.com)

### **Gregory Silberman**

Silicon Valley

+1.650.739.3954

[gpsilberman@jonesday.com](mailto:gpsilberman@jonesday.com)

### **Stefano Macchi di Cellere**

Milan / London

+39.02.7645.4001 / +44.20.7039.5959

[smacchi@jonesday.com](mailto:smacchi@jonesday.com)

### **Mauricio F. Paez**

New York

+1.212.326.7889

[mfpaez@jonesday.com](mailto:mfpaez@jonesday.com)

*The authors wish to thank Amir Amiri, an associate in the San Francisco Office, for his assistance in the preparation of this Commentary.*

Jones Day publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information purposes only and may not be quoted or referred to in any other publication or proceeding without the prior written consent of the Firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our "Contact Us" form, which can be found on our web site at [www.jonesday.com](http://www.jonesday.com). The mailing of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of the Firm.