Cornell International Law Journal Online

Google Paves The Way For Italian Internet Service Providers: Personal Data Protection In Italy

By Timothy Prosky*

Over the last twenty years, the use of the Internet has fostered innovation and creativity; it has also, through its open, decentralized nature, created communication channels throughout the world. However, the Internet's very nature necessitates governmental protection of personal information. The European Parliament and the Council of the European Union have been striving to achieve this necessary protection through a series of directives mandating member state Internet regulation. The continuous implementation of these directives helps the European Union (EU) achieve consistency when dealing with the complex issues that the ever-changing dynamic of the Internet presents. Current judicial rulings reflect the member states' efforts to adapt their legislation to emulate the directives set forth by the EU. This article analyzes a recent Italian Supreme Court decision interpreting the Italian Personal Data Protection Code; this decision is emblematic of Italy's attempts to tailor its legislation to the EU directives, and the gaps that still remain between EU mandates and Italian application.

Google v. Vividown

One of the most prevalent issues involving the Italian Personal Data Protection Code (IPDPC) is whether an Internet Service Provider (ISP) is required to protect a third party from having his or her personal data exposed on the ISP's platform.[1] On December 11, 2013, the Italian Supreme Court shed some light on this issue by affirming a Milan Court of Appeals ruling in a case between Google and Vividown.[2] The case first appeared in front of the Court of First Instance in 2010, where three Google executives were tried for unlawful data

* Timothy Prosky is a J.D. candidate at the Elon University School of Law. He graduated from the University of South Carolina with degrees in Accounting and Financial Real Estate.

[1] Cass. Pen., sez III, 3 febbraio 2014, n. 5107 (It.).

[2] *See id.*

processing.[3] These charges stemmed from a video posted by a Google user that depicted an autistic boy being harassed by a group of schoolmates in Turin, Italy.[4]

The Court of First Instance held that the executives were liable for unlawful data processing pursuant to section 167 of the IPDPC.[5] Section 167 states that "[a]ny person who, with a view to gaining for himself or another or with the intent to cause harm to another, processes personal data in breach of [sections within the IPDPC that require consent of personal data subjects] shall be punished, if harm is caused, by imprisonment."[6] The court held that a website operator "processes" data if the operator collects, processes, selects, uses or organizes the content that gets uploaded to their platform.[7] With so broad a definition, even mechanistic maintenance of Internet services was enough to create liability—and the court thus found the Google officers guilty of violating Italian law. The officers had failed to obtain the consent of the autistic boy or his guardians, they had processed the boy's sensitive personal data, and Google had the intent to profit from this personal data.[8]

On December 21, 2012, the Milan Court of Appeal overturned the lower court's decision.[9] The Court of Appeal's holding hinged on the determination that Google is a "passive" ISP, which means that it is not required to monitor the sensitive data that its users post to its platform.[10] A "passive" hosting provider does not process data; instead it "merely provide[s] hosting services without having any active role in managing the information stored on the relevant websites."[11] The Court of Appeals explained their reasoning, stating that "providing the tools" to process data is not the same as processing the data; rather it is the uploader of the data who actually processes the content.[12] Thus it

---

[3] Trib. Milan, 24 febbraio 2010, n. 1972 (It.), *available at* http://www.giurcost.org/casi_scelti/Google.pdf.
[4] *Id.*
[5] *Id.*
[6] D.Lgs. 30 June 2003, n. 196, § 167(1).
[7] Trib. Milan, 24 febbraio 2010, n. 1972 (It.).
[8] *See id.*; *see also* Noah Hampson, *Comment: The Internet Is Not A Lawless Prairie: Data Protection and Privacy In Italy*, 34 B.C. INT'L & COMP. L. REV. 477. (2011).
[9] *See* App. Milan, 27 febbraio 2013, n. 8611 (It.), *available at* http://www.openmediacoalition.it/documenti/app-milano-27-febbraio-2013-n-8611/.
[10] *See id.*
[11] Ernesto Apa & Federica De Santis, *ISP Liability For User-Uploaded Content – an Italian Perspective*, INTERNATIONAL BAR ASSOCIATION, *available at* http://www.ibanet.org/Article/Detail.aspx?ArticleUid=daa37c2d-68fc-4b7f-911f-ffa202c223d0 (last visited Apr. 13, 2014); *see also* Council Directive 2000/31, Directive on Electronic Commerce, 2000 O.J. (L 178) 7 (EC).
[12] *See* App. Milan, 27 febbraio 2013, n. 8611 (It.).

was the uploader's responsibility, not Google's, to obtain the boy's consent.[13] The Court of Appeal's decision not only narrows the broad language of the IPDPC, but also reflects the intent of an EU internet law directive stating that "[m]ember States shall not impose a general obligation on ["passive" hosting] providers to monitor the information which they transmit."[14] This ruling sets the precedent that it is the user of a "passive" ISP, not the ISP itself, who is subject to criminal liability under section 167 of the IPDPC when the user posts sensitive data of a third party without their consent.

On December 11, 2013, the Italian Supreme Court upheld the Court of Appeal's decision, reinforcing the ruling that ISPs are not responsible for sensitive data that is uploaded to their platform.[15] The court reasoned that Google has no control over the data stored, nor does it contribute in any way to the creation of the file; as such, Google is not within the scope of the penal sanctions of the IPDPC.[16] This outcome not only gives ISPs like Google confidence in the protections provided in Italy and the EU, but also alleviates concerns that the interpretation and implementation of the directives would restrict ISPs' ability to foster a free flowing system that allows its users to conveniently share information.[17]

While the decision by the Supreme Court provides a comprehensive overview of why Google is exempt from liability, the court failed to discuss Google's affirmative data protection responsibilities required by the EU directives. The directives place an obligation on a "passive" ISP to remove specified content upon notification by a competent authority, and it may be considered liable when it fails to comply with the order and remove the content.[18] The court's opinion here merely stated that if an ISP does not create or modify content on its platform, then it is not required to protect third party information, which fails to recognize the directive's affirmative obligation.[19]

---

[13] *Id*; *see also* Apa & De Santis, *supra* note 11.
[14] Directive on Electronic Commerce, *supra* note 11, art. 15(1), at 13.
[15] *See* Cass. Pen., sez III, 3 febbraio 2014, n. 5107 (It.).
[16] *See id.*; *see also Google vs. Vividown*, CUGI CUOMO & ASSOCIATI, *available at* http://www.cugiacuomo.it/site/news/english-google-vs-vividown/ (last visited Apr. 13, 2014).
[17] *See e.g.*, Rachel Donadio, *Larger Threat Is Seen in Google Case*, N.Y. TIMES (Feb. 24, 2010), *available at* http://www.nytimes.com/2010/02/25/technology/companies/25google.html? pagewanted=all&_r=0; *see also* Eric Pfanner, *Italian Appeals Court Acquits 3 Google Executives in Privacy Case*, N.Y. TIMES (Dec. 21, 2012), http://www.nytimes.com/2012/12/22/business/global/italian-appeals-court-acquits-3-google-executives-in-privacy-case.html.
[18] Directive on Electronic Commerce, *supra* note 11, art. 12, at 12-13.
[19] *See* Cass. Pen., sez III, 3 febbraio 2014, n. 5107 (It.).

The decision can be read as disregarding this aspect of the EU directive because it was not relevant to facts at hand — Google had no data protection responsibilities relevant to the facts. But when compared with the clarifications on the scope of processing, the court's opinion raises the question of whether Italian law totally tracks EU rules and requires passive ISPs to remove specified content upon notification. Either way, the court's failure to recognize the EU's affirmative obligation leaves some uncertainty as to the data protection responsibilities of a "passive" ISP. It falls to *Garante*, an Italian regulatory agency tasked with protecting personal data, to work through this judicial fog to determine the convergence of EU and Italian Internet regulation.[20]

Conclusion

The *Vividown* decision is one of Italy's the first critical decisions interpreting the duty owed by ISPs under both its own laws and the EU directives. It sets a pivotal precedent that ISPs' similar to Google are considered "passive" hosting providers, and are thus exempt from liability for a lack of third party consent. However, the court left much to be determined, as there are potentially other types of data where a host provider may have more affirmative duties. While the bounds of these responsibilities are still being determined, Internet providers can take some small comfort from the *Vividown* decision, knowing that the EU's directives are not intended to make ISPs monitor every piece of data uploaded to their platforms.

[20] D.Lgs. 30 June 2003, n. 196/2003, §§ 153-154.