# CHILDREN OF A LESSER GOD? THE VIVIDOWN CASE AND PRIVACY ON THE INTERNET

# FILHOS DE UM DEUS MENOR? O CASO VIVIDOWN E A PRIVACIDADE NA INTERNET

***Gianluca Andresani***
Durham University (United Kingdom)

***Natalina Stamile***
University of Bergamo (Università di Bergamo – UniBg) (Italy)

Recebimento: 14 jan. 2019
Aceitação: 4 jun. 2019

**Como citar este artigo / How to cite this article (informe a data atual de acesso / inform the current date of access):**

ANDRESANI, Gianluca; STAMILE, Natalina. Children of a lesser God? The Vividown case and privacy on the internet. **Revista da Faculdade de Direito UFPR**, Curitiba, PR, Brasil, v. 64, n. 2, p. 141-159, maio/ago. 2019. ISSN 2236-7284. Disponível em: https://revistas.ufpr.br/direito/article/view/64319. Acesso em: 31 ago. 2019. DOI: http://dx.doi.org/10.5380/rfdufpr.v64i2.64319.

## ABSTRACT
In the wake of high profile and recent events of blatant privacy violations, which also raise issues of democratic accountability as well as, at least potentially, undermining the legitimacy of current local and international governance arrangements, a rethinking of the justification of the right to privacy is proposed. In this paper, the case of the violation of the privacy of a bullied autistic youngster and the consequent prosecution of 3 Google executives will be discussed first. We will then analyse the arguments made by both academic experts and pundits who agree with Google's claim that if the first sentence had been left unchallenged, it would have opened the floodgates to several other jurisdictions that would as a consequence have used it as a pretext to increase control on the internet, jeopardising in such a way free speech, which has been seen so far as an inalienable right which *should* not be censored. Finally, by going beyond the sentences and their immediate contexts, we will propose a theoretical justification of our analysis. Our main claim is that the value of the right to privacy is based on the argument that its violation would undermine citizens' capacity to participate effectively in democratic politics.

## KEYWORDS
Jurisprudence. Human rights and democracy. Information technology law, ethics and governance. Privacy vs freedom of expression. Constitutional and legal rights.

## RESUMO
Na esteira dos recentes e importantes eventos de flagrantes violações da privacidade, é proposto um repensar da justificativa do direito à privacidade, pois tais violações levantam questões de responsabilidade democrática e, ao menos potencialmente, contribuem para corroer a legitimidade das atuais organizações de governança locais e internacionais. Neste artigo, discutir-se-á

* The authors are grateful for comments to William Lucy, Thom Brooks, Massimo La Torre and the anonymous reviewers.

primeiramente o caso da violação da privacidade de um jovem autista intimidado (*bullied*) e o consequente julgamento de três executivos do Google. Depois, serão analisados os argumentos dos especialistas, acadêmicos ou não, que concordam com a afirmação do Google de que, se a primeira sentença não tivesse sido contestada, as comportas para várias outras jurisdições teriam sido abertas e, como consequência, serviriam como pretexto para aumentar o controle na internet, comprometendo a liberdade de expressão enquanto direito inalienável que não *deveria* ser censurado. Por fim, além das sentenças e dos seus contextos imediatos, propõe-se uma justificativa teórica da análise exposta. O principal argumento consiste no valor do direito à privacidade estar baseado na leitura de que sua violação prejudicaria a capacidade dos cidadãos de participar efetivamente da política democrática.

**PALAVRAS-CHAVE**
Jurisprudência. Direitos humanos e democracia. *Cyberdireito,* ética e governança. Privacidade *vs* liberdade de expressão. Direitos legais e constitucionais.

## INTRODUCTION

In view of perceived regulation shortcomings, self-regulation as an alternative to Regulated Self-Governance (Andresani and Ferlie 2006; see also Knill and Tosun 2012) has been seen as a response both more effective and flexible. According to the literature, the growth and increasing liberalisation of international trade combined with the development of capital markets has resulted in a sort of 'governance deficit' (Newell, 2002). If trade and capital liberalisation are to be seen as important indicators of economic globalisation, with implications for business regulation and corporate governance (see Dignam and Galanis, 2008), CSR–induced initiatives have been considered as the remaining alternative in such a governance void, flexible enough to accommodate different jurisdictional and cultural contexts. In discussing the contribution of International Business Law and Ethics to business-governance issues under conditions of globalisation, the case of Internet Providers is particularly revealing. The recent Vividown case will be examined in order to assess if self-regulation and 'light' (Network) Governance is and *should* always be the right regulatory approach (Andresani and Ferlie 2006, Ferlie, Musselin and Andresani 2012). In fact, the prosecution of 3 Google executives for the delay in removing from their Italian site a video portraying an autistic youngster being bullied has interesting implications for the debate on the influence of formal and informal institutions on organisational behaviour. As Le Menestrel et al. (2002) have shown regarding a similar case, Yahoo! did not see fit to remedy the problems indicated by the activists, revealing a different understanding of freedom of expression which reflects different institutionally-embedded social expectations. Similarly, in the Google-Vividown case, only after the Italian courts intervened the internet provider giant started to address issues of e-ethics (e.g. Kafka, 2010). The problem is quite thorny. On the one hand, modern communications networks, including Internet, seem to use the

same expressions and the same type of 'hate speech'. In this perspective, technologies assume, in general, the aspects of 'mere tool' to spread already entrenched biases and prejudices (such as homophobic and racist speech). On the other hand, networks facilitate the manifestation of hate speech. In this latter case, Internet is not only a tool, but it is able to act as a sort of 'multiplier' by expanding and stimulating new and old types of behaviour thanks to specific psychological mechanisms ('crowd effects, 'distance' etc). So, Internet is not 'neutral', but it contributes to create an environment in which inhibitory mechanisms are lowered (Ziccardi 2016, see also Andresani and Stamile 2018).

In this paper, we will use both arguments and narratives (Andresani and Ward forthcoming) to show that the case has wider implications not only for comparative institutional analysis (cf. Doh and Guay, 2006; Matten and Moon, 2004), but also for legal and philosophical reflections.

## 1 BACKGROUND OF THE CASE

The Vividown case is about an incriminated video that shows an autistic student being bullied by a few teenagers amongst the indifference of other schoolmates in a secondary school in Turin. The disabled teenager is seen subjected to psychological and physical harassment: objects are thrown at him and as a consequence his glasses drop on the floor. He is portrayed bending and looking for them while a student insults him as well a voluntary association (Vividown, from which comes the name of the case and which deals with disabled persons affected by Downs Syndrome) in a mock phone call. Another student is seen recording and a third one drawing an 'SS' sign on the blackboard and with the arm raised in the Roman salute. The video was recorded at the end of May 2006, uploaded onto Google Video on September 8th and remained available online until November 7th before being removed (see Repubblica, 2010). The video became highly ranked in the "funny video" category, reaching more than five thousand downloads. Through the use of Google Ad-Words services, some specific terms began to be associated with the video: advertising posts thus appeared beside the images. An act of violence and crude disrespect thus apparently turned into a business affair. More precisely the video had a duration of about 3 minutes and at certain point it was possible to listen the Italian offensive expression: "mongolo", normally used to indicate people affected by Down Syndrome. (See: Sentenza di primo grado, Sentenza n. 1972/2010. Tribunale Ordinario di Milano in composizione monocratica. Sezione 4 Penale).

Three Google executives were prosecuted for violation of the Italian law on privacy while being cleared together with another regional marketing manager of the defamation (libel) charge on

February 24th 2010. This first sentence caused strong reactions. A Google representative stated that they would appeal against the sentence, as they did, because it was a threat against freedom of expression. The American ambassador in Rome also expressed his uneasiness with the sentence based on similar arguments.

## 2 SECOND AND THIRD SENTENCES

A different view was that of the court of second instance, in 2012. In fact, its decision completely overturned the previous judgment by pointing out that: "Art. 167 of Legislative Decree n. 196 of 2003 does not refer to the previous article n. 13 and, therefore, does not require the Internet provider to inform the user about the existence and content of the privacy laws. In fact, any violation of the cited art. 13" refers "not to art. 167, but art. 161" (cf. Corte di Appello of Milan, December 21, 2012). The key point is that the *Corte di Appello* decided to exclude the existence (*dolo specifico*) as it was attributed to the defendants in the previous sentence[1]. The obligation to provide information rests therefore on the uploader, and not on the third party[2]. In fact, the Court said that the specific intent may not "be considered as coinciding with the end of profit" because art. 167 "postulates the necessary psychological intentional participation […] to achieve a profit" (cf. Corte di Appello of Milan, December 21, 2012). But, beyond the enthusiasm that followed the acquittal, this second sentence raised many controversies, which were fuelled even more by the judgment of the *Suprema Corte di Cassazione*, III sezione penale, n. 3672, whose sentence was filed on February 3, 2014.

In this last sentence, the judges did not depart from the judgment of the Court of Appeal, and stated that the hosting provider would not be able to monitor all content uploaded to the network. To sum up, in the final sentence the court considered the second sentence as justified, after having analysed every point raised in the appeal. So, the internet hosting provider, according to article 16 of Legislative Decree n. 70 of 2003, "has no control over the storing of data […], since the data are entirely attributable to the user receiving the service as he (or she) uploads them on the platform placed at his disposal" (cf. Corte di Appello of Milan, December 21, 2012).

The internet hosting provider, then, would not be liable for storing information at the request of the recipient of a service if two conditions occur: first, that the provider does not have knowledge of illegal activity or information. Second, that as soon as it was made aware of the illegality, upon

[1] Regarding the technical aspects of *dolo specifico* and *dolo eventuale* see Mantovani (2013) and Fiandaca and Musco (2010). Note also that in this article all translations from Italian are ours.
[2] See art. 167 of Legislative Decree n. 196 of the 2003 Privacy Code.

notice by the competent authorities, the provider did act immediately to remove the data. Thus, Google Video, as a *mere instrument*, was considered as a simple platform where the person responsible is the one who uploaded data on it[3]. This interpretation of the *Corte di Cassazione* would seem to comply with that affirmed in the European Directive 2000/31/CE and article 17 of the Legislative Decree 70 of 2003 (the Electronic Commerce Code) "that excludes […] a general obligation to monitor the information transmitted or stored, and a general obligation to seek actively any crimes"[4]. This element should be identified as "the point of balance between the freedom of the provider and the protection of persons who eventually may be damaged by making available the information[5]. This last sentence also raised strong reactions.

## 3 ANALYSIS OF THE CASE

This case is relevant for several reasons. First, because several pundits agreed with Google's argument about the attack to free speech involved in this case (Whitcomb, 2010). It is also important to point out that the judge of the first trial, in justifying the sentence focused on (the breach of) the right to privacy, which is protected by the Italian law, apparently gave priority to it in his judgement *vis-à-vis* freedom of expression[6]. So what to make of this case? Who is right: Google or the Italian judge of the first court?[7] The striking characteristic of this case is that it has several implications which go well beyond those specific to the first sentence and its immediate context.

## 4 THE SPECIFICITY OF THE INTERNET

Google executives find themselves in the unlikely position of being heralded as the paladins of free speech and human rights, and the Italian judge and prosecutors of the first court as medieval witch-hunters trapped in an antediluvian ideology[8]. We will consider the details of the case in the next section, but here we just want to indicate that it is not surprising that blogs and media reacted through vivid stories as well as arguments in such a strong manner, to the extent that the New York Times claimed that "(t)he verdict, though subject to appeal, could have sweeping implications

[3] Cf. Corte di Appello of Milan.
[4] *Ibidem.*
[5] *Ivi*, 11. See also Court of Justice regarding Case C-131/12. *Ivi*, 12.
[6] Tribunale di Milano, 12 April 2010 n. 1972.
[7] In this article our focus is primarily on the arguments and narratives regarding the first sentence.
[8] This must also be seen in the context of the controversies on Streetview and Buzz: see e.g. Guardian, (2010); Barber and Palmer (2010).

worldwide for Internet freedom" (Donadio, 2010). Judge Oscar Magi in an interview complained that he had even received threats and insults via email and on his Facebook pages[9]. In fact, what could be more threatening than an assault on the virtual agora? As Google stated in their blog, the ruling in the first sentence "attacks the very principles of freedom on which the Internet is built" (Googleblog, 2010). The main argument is that internet is a new medium, self-regulating and *intrinsically* democratic: surely any attempt to transpose the *old* ways of thinking (including *old* ethical arguments) to a *fundamentally* new technology and medium is to be judged at best as naïve and at worst as authoritarian. Technological innovation creates new possibilities for human action, the argument goes, which poses entirely new questions and ethical issues. Oscar Magi clearly states in motivating the 3 six-month suspended sentences for violation of privacy that the internet instead "is not a borderless grassland where everything is allowed and nothing is forbidden" (Tribunale di Milano, 12 April 2010 n.1972, p. 98). This is the first ethical issue to be addressed: is the internet something *fundamentally* new which requires new ethical principles and arguments or not?

It is possible to find support for both positions in the literature on internet and e-ethics. There is no doubt that new issues and an entire field (computer and/or internet ethics) has emerged because the internet is indeed a new medium and technology. It is apparent that the internet revolution revolves around a specific novelty: users of the internet can express their opinion for the first time *without* intermediaries. That was and still is not possible for users of other media such as newspapers or TV programmes. As a consequence, how can internet (service and/or content) providers (IPs) be held legally and morally liable in the same way as editors of newspapers or TV programmes are? This is a big issue and if anything the Vividown case has at the very least inspired a much needed debate. The first aspect is: is it *technically* feasible to control the contents put on the space that providers make available? The second: *should* IPs such as Google control them?

As Oscar Magi explains in the first sentence[10], by indexing the content of the videos, notwithstanding their denial, Google is technically able to do that: the very way AdWords works is based on the fact that it *is* possible to examine contents. This is how Google is able to make profits: the ads that appear after a user has carried out her search are *linked* to the content of the results of the search. From clicking on the ads, Google has been able to exploit commercially what at first was seen as an unprofitable enterprise[11]. There is also no doubt that Google is able to *filter* and therefore examine the content, as they have admitted during the Chinese debacle (Smith, 2009 and Brenkert,

[9] Sole24, (2010).
[10] Cf. Tribunale di Milano § 9, 62 ff.
[11] *Ivi*, 63-64.

2009). In the sentence, it is even suggested that just a check on the title of the incriminated video would have sufficed to spot its problematic content, because it contained offensive language and hate speech. Other suggestions can be extrapolated by examining the number of hits that videos have: the higher the number of hits, the more appropriate it would be to check (manually) its content. As a matter of fact, the video was widely viewed, it was ranked first of the funniest videos list as well as being ranked amongst those most clicked. Still, this is a controversial issue: Google and other internet providers can operate by relying on automating as many as possible of their operations (Edwards, 2010). They have built their commercial success on that. The more they rely on manual processes (i.e. involving human scrutiny), the less profitable they are. It seems (and this is the argument of Oscar Magi and the Italian prosecutors in the first trial) that it is indeed technically feasible. So since it is technically possible to control contents, would it be *ethically* appropriate (Donadio, 2010)?

We have to turn now to the specificity of e-ethics. This is another contested topic, and we will use the case again as a way to shed lights on some of the issues involved. After having admitted (as we did above) the novelty of the internet, the next step would be to consider how we should address the ethical issues it raises. Shall we throw away all old principles, values and arguments and start a new when we address issues of e-ethics? We agree with Deborah Johnson (2001) on giving a genus-species account. The novelty of the internet (and the field of computer or e-ethics) requires that we address these new issues by drawing analogies from *old* or, more correctly, different areas, where principles and arguments proved to be appropriate and indeed useful. Computer and internet ethics issues should be approached as new *species* of familiar (*generic*) moral issues. This meta-ethical claim is based on the denial of technological determinism: i.e. the assumption that (new) technology cannot impact on us in such a way as to create an entirely new ethical landscape. We cannot even recognise an ethical problem as such unless we are able to connect it to familiar ethical concepts and issues. The case put an emphasis on the question if there are situations which we would categorise as unethical in *familiar* circumstances, but that should *not* be judged as such in virtual conditions. Hate speech and especially harassment are (known to be) not acceptable in familiar situations, why should they be accepted on the internet?

Let's assume (and we do assume that) that it is not acceptable (but this is not universally agreed), then what should be done about it? Should we censure the internet? The implication of not accepting harassment on the internet is that some form of control should be put in place. A similar case of cyberbullying caused outrage in Australia, where Facebook pages set up in tribute of two

murdered children were inundated with pornography and obscenities[12]. Facebook's reply to the strong criticisms (coming also from political quarters) about the fact that they allowed that outrage to happen was the standard one which was also to be relied upon in the Vividown: that the net is able to self-regulate. As soon as they receive(d) notice (from other internet users) a (the) problematic content is (was) quickly removed. But what if that doesn't not happen *quickly*? After all, in the case we are examining here the video was publicly available for two months. One could argue that after about a month users did manifest their disgust by writing comments below the video in the comments section. Assuming that there is a technically feasible way of spotting and removing the content quickly after the notice has been received (as argued above, whether by using an automatic or manual procedure), still users did not ventilate their unease for about a month. Moreover, the video was indeed removed quickly (within hours of being notified), but the only *notification* that Google paid attention to was the one they received by the Italian police following the charge made before them by Vividown (which for the *Corte di Appello* and *Corte di Cassazione* was enough). If anything, the case shows that self-regulation might not always work. The case rightly indicates that internet providers should address the issue instead of ignoring it otherwise the internet as we have known it so far could indeed be under threat.

Let's now address the issue of when, if ever, should content be controlled: *before* or *after* being made available on the net? Before answering the question it is necessary to look briefly into the *technical* aspects again. Solutions to the problem can indeed be found, such as improving the flagging system: i.e. there should be no need to register to flag a content as inappropriate (as it was required by YouTube) because this might put users off and as a result Google should *invest* in units staffed by employees who would quickly check notices and remove contents if inappropriate. Once a feasible solution has been found, our view is that it is much more problematic to rely on *preventive* control. It would bring us back to the Chinese filtering scenario. In fact, judge Magi does not advocate it in the sentence. Still, even if the control is *post-hoc* (as a consequence of flagging or a notice), the problem of how to decide what is *inappropriate* remains (see also Gunther 1992): what criteria should be used to label contents as inappropriate?

[12] See also note 9 above.

## 5 DIGNITY VS LIBERTY

The case seems to give a hint as to how the question above should be answered: all content that breaches the law(s) of the land should be removed. This is not a satisfactory answer, because it would justify censorship of the kind currently carried out in China again. What ethical criteria should be used rather than focussing solely on the legal ones then? We enter here into the murky territory of international legal theory. The question should then be reworded as such: are there universal ethical criteria that businesses/governments should adopt in all circumstances and geographical/cultural contexts? This is another tricky issue and we do not pretend to solve it here. Rather, we will stick to the case and examine its implications for current debates (see also Andresani 2019). To begin with, the actors involved have themselves categorised the differences in the interpretation of the case as a trade-off between freedom of expression versus the right to privacy. According to Goggle's CEO Eric Schmidt, the troubles coming from accusations of violation of privacy which have caused so many headaches to the company recently (i.e the Streetview, Buzz, Vividown) are due to the fact that their organisational culture put an emphasis on creativity. He argues that "the 'launch first, correct later' approach is vital to the ultra-creative and flexible company… (His) remedy is to protect the company's freewheeling culture, while adopting a rigorous policy of owning up to mistakes and correcting them. That might mean more lawyers and more privacy briefings, but the engineers must be given space to work their software magic" (Barber and Palmer, 2010).

Not only he labels the Vividown's sentence as "bullshit" (*verbatim*), but he clearly shows his uneasiness with addressing issues of privacy, which if properly handled would jeopardise the creativity that he believes is the *magic* source of the company's success.

Here, creativity and freewheeling culture seem to stand for prioritising freedom of expression *vis-à-vis* the right to privacy. Alfredo Robledo, one of the two prosecutors in the Vividown case, is more explicit in construing the *querelle* between an emphasis on freedom of expression versus the human right to privacy. To the question that Google accuse them of using privacy as a pretext to introduce censorship, Robledo replies:

> The first amendment of the American constitution puts freedom of expression above any other statutory initiative, but the American constitution is a local statute. **Question**: **Local?** Yes. In Italy and Europe freedom of expression is bounded by the respect for human rights [literally, persons' rights, i.e. subjective rights, G. A. and N. S.], amongst which stands out that to privacy. Google can't continue to ignore this (Mucchetti, 2010).

At first sight the solution to the dilemma is straightforward: the right to privacy is neither absolute nor necessarily inalienable. According to Spinello, "(it) is limited by other rights and moral

considerations because some conditions override the right to privacy" (Spinello, 2010, p. 379).

Moreover, as Hilary Clinton stated – quoted by the American ambassador in Rome while expressing his disappointment for the sentence – "free Internet is an integral human right that must be protected in free societies"[13]. So, some strong negative reactions and narratives as well as outlines of arguments from the blogosphere (see Gilioli, 2010; Kafka, 2010; Whitcomb, 2010; also Moore 2000) and the recognition by (some) computer and internet ethics experts such as Spinello that the right to privacy is a claim right subordinate to other rights[14], such as freedom of expression and speech, seem to settle the controversy. Since the enormous literature on rights, including the one focusing specifically on (human) rights in relation to institutional ethics (Campbell and Miller, 2004) has shown that there is or should be an ethical discussion around which right(s) should prevail on other right(s) in specific circumstances, and since the right to privacy has been *conceptualised* as *potentially* subordinate to other (higher order) rights such as freedom of expression, surely Google must be right and the Italian judges wrong (see also Rosenberg 1999).

First, the right to privacy has not been theorised as subordinate by all scholars, including computer and internet ethics experts. Deborah Johnson (2001), as Spinello (2010) acknowledges, is of the opinion that the current debate around the right to privacy should be reconsidered, so that it could be indeed reconceptualised as a *Fundamental Legal Right*[15]. The fact that she finds herself in a minority position surely cannot *ipso facto* undermine the strengths of her arguments, if ever this could be considered as a criterion to assess reasons (although some sociologists of knowledge might disagree here). Furthermore, it is necessary to consider the institutional aspect: there is a clear Atlantic divide regarding how to judge privacy, which has been widely discussed. In fact, Whitman (2004) argues that such a divide has profound historical roots: the Europeans' focus on dignity comes from historical events that have shaped France and Germany which have led (the European continent) to

[13] DONADIO, R. (2010).

[14] See Etzioni (1999 in Norman and Jamal, p. 323): "Most people support a right to privacy. Philosophers have provided a number of arguments that justify a right to privacy although there are certain situations where many would agree that privacy rights need to be sacrified either in order to honor other rights or for the general public good". Also Norman and Jamal (2006, p. 324): "with internet and the development of marketing by e-commerce, privacy issues became more complicated as a result of new technology".

[15] See especially Peslak (2005); also Bowie and Jamal (2006, p. 324-326), for a Kantian justification of the right to privacy: "Joseph Kupfer (1987) has argued that privacy is a necessary condition for the development of autonomous selves […] Privacy is necessary for an efficacious self-concept and an efficacious self-concept is in turn required if one is to be an autonomous self" (p. 325). But they recognise also that "Despite the value of privacy to the development of an autonomous self-concept, we recognize that the right to privacy is not absolute […] we do not think the central moral issue is the importance of the information but rather who has a moral right to the information whatever the importance of it" (p. 326-327). Finally see Introna and Pouloudi (1999, p. 27).

put particular emphasis on 'honour' and as a consequence privacy[16]. This is difficult to understand in the USA because of a different historical trajectory (*path dependence*), with a consequent emphasis over there on a Lockean conception of freedom and the supremacy of the first amendment (read: freedom of expression). Indeed, the *discovery* of a right to privacy came quite late (Warren and Brandeis, 1890). It seems then that Robledo has pointed out to a real issue. But, how could such an *institutional* awareness help in the Vividown case? One route would be the one suggested by Brenkert (see Brenkert, 2009, also Smith 2009): assuming that Google feel so strongly about freedom of expression (and again their involvement in censorship in China seems to indicate otherwise), would then reflecting on the possibility of compromising their values be the way forward or at least the lesser evil in this case? True: Brenkert refers to the difficult situation Google found itself in China, where it had to face the hard choice between withdrawing from China and compromising its values by accepting Chinese authorities' imposition of authoritarian constraints on internet freedom. Brenkert's complex argument is that in real life we need indeed to make compromises when dealing with hard (ethical/legal) cases, such the one Google faced in China. But the fact is that it dwindled quite a lot in the Chinese case: at first, it did compromise its values until the case exploded in the (Western) media. Under huge pressure, it decided that (compromise) was not a satisfactory (for Google) choice and, as a consequence, it seemed to prefer to remain *truer* to its motto, 'do no evil', and decided instead to resolve the stand-off with Beijing by moving its operations to the more liberal Hong Kong, while at the same time refusing to be involved anymore in internet censorship. Eventually, it was clear that was a temporary solution, since it did return to (mainland) China and, in any case, during the time it moved to Hong Kong, filtering remained in place for searches carried out from mainland China (Warburton, 2010).

The reactions so far (including the one in the FT interview of Google's CEO mentioned above) seem to indicate that compromising (assuming that *integrity* is what Google are interested in this as well as in the other cases) is quite unlikely to be the option that they will consider. But, *should* they compromise or, better still, reconsider the *priority* they have given to freedom of expression so far (or, more accurately, until it seems to be convenient to their economic interests), particularly when compared to the right to privacy? When one reviews the literature on international institutional (business) law and ethics, work that focuses particularly on human rights seems to give no definitive answer (Beauchamp, 2010; Campbell and Miller, 2004). Even if we adopted some form of *thin* universalism, as suggested by Beauchamp (2010, see also Arnold et al 2013), for example, we could

[16] It is not necessary for the argument to address here the convoluted legal heritages: which national culture influenced the other ones first? See also Zucca (2007).

not avoid addressing the peculiarities of the ethical situation, which would lead consequently, and *rightly*, to a focus on the specific characteristics of the case (see also Andresani and Ward forthcoming). As far as protecting the weak party is concerned - and in this case there is no doubt that a bullied disabled boy is the weak party when compared to a powerful multinational company –, the right to have his privacy protected would indeed trump the right to have freedom of expression (read: private property) safeguarded. Accepting to constrain the freedom of expression/enterprise they (Google) have enjoyed so far, in order to protect the right to privacy of individuals (i.e. citizens such as consumers, employees, etc), would indeed be the right step towards an international debate on *institutional diversity*, aimed at reconsidering and addressing the *excessive* power that (large) companies still enjoy in the US legal system when compared to more (social) democratic jurisdictions (e.g. Europe), where citizens' rights are in general *protected* from (violation by powerful) private as well as public actors. The key point here is that a stronger reliance on governance (i.e. political and legal regulation of businesses, particularly by relying on the political and economic *clout* of the EU) should be contemplated if required in such cases where the (economic) interests of *very* powerful actors such as Google are judged – as a result of democratic *deliberation* – to be subordinate to the (privacy) rights/interests of (much weaker) citizens. It is simply not possible to rely *exclusively* and indeed prominently on self-regulation (Pace Dignam and Galanis (2008); see especially Aglietta and Rebérioux, 2005). Furthermore, Google's 'do no evil' motto would for sure go against any attempt to put aside ethical concerns as irrelevant in the economic realm[17]. Now, as we suggested above, this would not require *trickier* constraints such as preventive controls of contents. The effort here seems to be more an *economic* one of *investing* in processes (that would involve the scrutiny of contents as a consequence of notice of violations of privacy) that would *better* protect privacy. The *post-hoc* checks would only focus on violations of privacy (a very limited aspect) and could be implemented by considering some combination of the technical solutions discussed above and as a result of working in partnership with the Italian Privacy Authority. As Magi argues in the sentence[18], Google *deliberately* ignored so far the concerns that *l'autorità garante per la protezione dei dati personali* had repeatedly ventilated regarding indeed privacy issues.

This indicates in fact an *institutionally specific* solution to an *objective* moral dilemma. We could consider a specific hypothetical scenario as another illustration: if a Western company moves a branch to an Islamic country and it is faced with the request from its female employees to wear the

[17] See for a powerful rebuttal of the argument: Sen (1993), also Calabresi (1996); Tincani (2016); Lyon (1994); Solove (2002 and 2011); Thomson (1984); Richards (2015).
[18] Cf. Tribunale di Milano § 5, 52 ff.

veil at the workplace, leaving aside if it is required by the local laws that the company must comply with the request, it is the *right* decision to accept the request. Of course, it would be necessary to look at the specificities of the moral situation, but *in principle* there would be no particular difficulties involved in satisfying such a request.

Finally, as far as the public policy implications are concerned, ethical and political issues must also be faced. This case shows that a coordinated legislative solution, such the GDPR at the European level, goes in the right direction. At the time of the first sentence legal protection ("the safe harbours") for hosting intermediaries was guaranteed by the E-Commerce Directive (particularly articles 12-15) which was applied throughout Europe. But it did not safeguard adequately European citizens from privacy violations. In fact, the case has shown (and the first sentence also explicitly mentions) that a better legal solution for protecting privacy could and *should* be found also outside Europe, e.g. in the US[19]. Such a task has become even more urgent in view of the governance *deficit* (Newell, 2002) represented in the case here examined by the struggle that legitimately created laws (and democratically elected governments) have to endure when facing powerful (and unelected) private actors[20].

## 6 A RESOLUTION OF THE CONFLICT BETWEEN PRIVACY AND FREE SPEECH?

Our proposal then is that only the deontological structure provided by constitutional rules (Habermas, 1996) would not ostensibly violate the pluralistic tenets of political liberalism and (deliberative) democratic politics. Such structure, as advocated by a constructivist conception of *reflexive* law (Fleming, 2004 and Habermas, 1996), would instead allow a pragmatic judgment of *stricto sensu* conflicts of Fundamental (or Constitutional) Legal Rights (Alexy, 2002), and at the same time acknowledge their deontological justification. As we have seen in the analysis of the Vividown case, such a framework would indicate the following conclusion: the fundamental legal right to privacy is weightier than the fundamental legal right to free speech *in this case*. This is because of the *internal* rule of its substantive priority[21]. In fact, the fundamental legal right to privacy has a *qualified* priority in view of the type of considerations discussed in the case. Both fundamental legal

[19] Pace Bowie and Jamel (2006, p. 323): "we believe that insufficient evidence exists to propose formal government mandated internet regulation".
[20] See also Lipinski (1999, p. 63): "the boundary between private information, that which is owned, and public information, that which is deemed available for citizens to use free from proprietary is delicate. […] This delicate balance is related to the character of the information itself: digital information is mutable and is not bound by physical dimensions it is natural that others should attempt to establish others sorts of boundaries or limits upon its use".
[21] See Zucca (2007), who has the opposite view regarding the priority of privacy though.

rights express the recognition of a person's *status* (Kamm, 2002) as a being who has a high level of *inviolability* (Nagel, 1995 and Habermas, 1996). But such inviolability is not absolute, and therefore in our view balancing is possible (Alexy, 2002). To sum up, privacy enjoys a *qualified* priority which means that in other cases (certainly not the Vividown), other considerations might well overrule that priority. The introduction of such qualification would therefore avoid the problems associated with the *categorisation* strategy (Scanlon, 2004; Fleming, 2004 and Habermas, 1996).

Further research would need to analyse cases of *lato sensu* conflicts: e.g. the one between a fundamental legal right such as privacy and a collective goal such as security. In such cases, we would argue that privacy would enjoy again a *qualified* priority. This time, because of the *external* rule of substantive priority of fundamental legal rights (Habermas, 1996 and Zucca, 2007). The system of fundamental legal rights has, in fact, a *qualified* priority over any other type of considerations, which are external to them, such as the public interest to national security, due to their *inviolability*. Therefore, future research will have to answer this question: would a careful analysis of cases such the NSA warrant the overruling of the *qualified* priority enjoyed by the fundamental legal right to privacy?[22]

## 7 CONCLUDING REMARKS

In conclusion, the examination of arguments and stories in the Vividown case has shed a penetrating light on issues of Constitutional, IT and Business Law as well as Institutional and Internet ethics. The differences in the perceptions of the stakes involved do indeed reflect different and institutionally embedded expectations. It has been shown that, in order to uncover the issues surrounding the (mis)understanding of the protection of privacy, linking philosophical to institutional analysis would be a promising path to undertake (Habermas 1996). Attempts have been made to link both[23] but they have been carried out by economist and/or social (political) scientists addressing normative issues from a *social scientific* point of view. The challenge is to address normative issues from a philosophical point of view, while drawing upon the rich evidence provided by the social sciences, as in the best tradition of the application of political and legal philosophy to business and internet ethics. A promising route for further investigation in order to widen the results of this study

[22] Our claim in Andresani 2016 (see also Andresani and Stamile 2016, 2017) is that the answer is negative. As a commentator has rightly pointed out regarding the emergency legislation rushed through by the British government for security reasons: "Not only […] the proposed legislation infringe our right to privacy, it […] also set a dangerous precedent where the government simply re-legislates every time it disagrees with a decision by the CJEU… Blanket surveillance needs to end. That is what the court has said" (https://bit.ly/2ZU6Dre). See also Bernal (2014).
[23] E.g. the Regulation School: see Aglietta and Rebérioux (2005); also Matten and Moon (2004); Moon et al. (2010).

would be to see how an expanded *institutionally-focused* political and legal philosophical analysis would contribute to the previous discussion. Luckily, there are indeed signs of such an endeavour recently and currently being carried out (e.g. Hartmann, 2001; Moriarty, 2005; Heath et al., 2010).

## REFERENCES

AGLIETTA, M. and REBÉRIOUX, A. (2005). *Corporate Governance a Drift: A Critique of Shareholder Value*. Cheltenham, U.K.; Northampton, Mass.: Edward Elgar.

ALEXY, R. (2002). *A Theory of Constitutional Rights*. Oxford: Oxford University Press.

ANDRESANI, G. (2016) "The (In)Security State: Political not Existential", paper presented at the ERCS (The Common Good: Ethics and Rights in Cybersecurity) major conference 'Cybersecurity Ethics: The Common Good and the Digital Commons as Justification Registers in Digital Governance, Surveillance and Security', funded by the ESRC, Hull, UK, 20-21 October.

ANDRESANI, G. (2019) "A Defence of Digital Rights and Values", paper presented at the 'Human Rights in a Changing Context' conference, Durham, UK, 9-10 May.

ANDRESANI, G. and FERLIE, E. (2006) "Studying Governance within the British Public Sector and without: Theoretical and Methodological Issues", *Public Management Review*, Vol. 8, No. 3, pp. 415-431.

ANDRESANI, G. and STAMILE, N. (2016) "It's a Bad World Out There! Taking Liberty (Out)With Emergency" presented at the ERCS/International Association for Media and Communication Research (IAMCR) pre-conference workshop 'Surveillance and Security in the Age of Algorithmic Communication', Leicester, 26 July.

ANDRESANI, G. and STAMILE, N. (2017) "Legal Reasoning to the Barbed Wire", paper presented at the International Conference on Artificial Intelligence and Law (ICAIL), King's College, London, 12-16 June.

ANDRESANI, G. and STAMILE, N. (2018) "Transparency in Internet Regulation and Governance: Arguments and Counter-Arguments with Some Methodological Reflections", *RBEP*, 117, pp. 443-476.

ANDRESANI, G. and WARD, T. (forthcoming) "Arguments and Stories in Legal Reasoning: The Case of Evidence Law", *ARSP*.

BEAUCHAMP, T. L. (2010). *Relativism, Multiculturalism and, Universal Norms: Their Role in Business Ethics.* In G. G. BRENKERT and T. L. BEAUCHAMP (eds.), The Oxford Handbook of Business Ethics, (pp. 235-266). Oxford: Oxford University Press.

BERNAL, P. (2014). *Internet Privacy Rights.* Cambridge: Cambridge University Press.

BOWIE, Norman E. and JAMAL, Karim (2006). "Privacy Rights on the Internet: Self-Regulation or Government Regulation?", *Business Ethics Quarterly,* Vol. 16, No. 3, pp. 323-342.

BRENKERT, G. G. (2009). "Google, Human Rights, and Moral Compromise", *Journal of Business Ethics*, 85(4), pp. 453-478.

CALABRESI, G. (1996). *Il dono dello spirito maligno. Gli ideali, le convinzioni, I modi di pensare nei loro rapporti col diritto*. Milano: Giuffrè.

CAMPBELL, T. and MILLER, S. (eds) (2004). *Human Rights and the Moral Responsibilities of Corporate and Public Sector Organisations.* Dordrecht: Kluwer Academic Publishers.

DALTON, Dan R., WIMBUSH, James C. and DAILY, Catherine M. (1996). "Candor, Privacy, and 'Legal Immunity' in Business Ethics Research: An Empirical Assessment of the Randomized Response Technique (RRT)", *Business Ethics Quarterly*, Vol. 6, No. 1, pp. 87-99.

DENIS, G., BOWIE, N., BEAUCHAMP, T. L. and ARNOLD, D. G. (eds) (2018). *Ethical Theory and Business.* Cambridge: Cambridge University press.

DIGNAM, A. and GALANIS, M. (2008). "Corporate Governance and the Importance of Macroeconomic Context*", Oxford Journal of Legal Studies*, Vol. 28, No. 2, pp. 201-243.

DOH, J. P. and GUAY, T. R. (2006). "Corporate Social Responsibility, Public Policy, and NGO Activism in Europe and the United States: An Institutional-Stakeholder Perspective", *Journal of Management Studies*, Vol. 43, No 1, pp. 47-73.

ETZIONI, A. (1999), *The limits of Privacy*. New York: Basic Books.

FERLIE, E., MUSSELIN, C. and ANDRESANI, G. (2012) "El pilotaje de los sistemas de educación superior: una vision desde la perspective de la gestion publica", in KEHM, Barbara M. (ed.), *La nueva gobernanza de los sistemas universitarios.* Barcelona: Octaedro.

FIANDACA, G. and MUSCO, E. (2014). *Diritto penale*. Parte generale. Bologna: Zanichelli, 7th ed.

FLEMING, J. A. (2004). "Securing Deliberative Democracy", *Fordham Law Review*, 72, pp. 1.435-1.475.

GUNTHER, K. (1993) *The Sense of Appropriateness: Application Discourses in Morality and Law*, New York: State University of New York Press.

HABERMAS, J. (1996). *Between Facts and Norms, Polity.* Cambridge: Polity Press.

HARTMAN, E. M. (2001), "Moral Philosophy, Political Philosophy, and Organizational Ethics: A Response to Phillips and Margolis", *Business Ethics Quarterly*, Vol. 11, No. 4, pp. 673-685.

HEATH, J., MORIARTY, J. and NORMAN, W. (2010), "Business Ethics and (or as) Political Philosophy", *Business Ethics Quarterly*, Vol. 20, No. 3, pp. 427-452.

INTRONA, L. D., POULOUDI, Athanasia (1999). "Privacy in the Information Age: Stakeholders, Interests and Values", *Journal of Business Ethics*, Vol. 22, No. 1, Ethics of Information and Communication Technology, pp. 27-38.

JOHNSON, D. (2001). *Computer Ethics*. London: Prentice Hall International, 3rd ed.

KAMM, F. M. (2002). *Rights, in Coleman, J. and Shapiro, S. The Oxford Handbook of Jurisprudence and Philosophy of Law,* Oxford: Oxford University Press.

KNILL, C., TOSUN, J. (2012). *Public Policy: A New Introduction.* Basingstoke, Hampshire: Palgrave Macmillan.

LE MENESTREL, M., HUNTER, M. and BETTIGNIES, H.-C. de (2002), "Internet e-ethics in Confrontation with an Activists Agenda: Yahoo! on Trial", *Journal of Business Ethics*, Vol. 39, No. 1-2, pp. 135-144.

LIPINSKI, T. A. (1999) "The Commodification of Information and the Extension of Proprietary Rights into the Public Domain: Recent Legal (Case and Other) Developments in the United States", *Journal of Business Ethics*, Vol. 22, No. 1, Ethics of Information and Communication Technology, pp. 63-80.

LYON, D. (1994). *The Electronic Eye. The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.

MANTOVANI, F. (2013). *Diritto Penale*. Parte generale. Padova: CEDAM.

MATTEN, D. and MOON, J. (2004). "A Conceptual Framework for Understanding CSR in Europe", in HABISCH, A., JONKER, J., WEGNER, M. and SCHMIDPETER, R. (eds), *CSR across Europe* (pp. 335-356), Berlin: Springer.

MOON, J., KANG, N. and GOND, J.-P. (2010). "Corporate Social Responsibility and Government", in COHEN, D., GRANT, W. and WILSON, G. (eds.), *The Oxford Handbook of Business and Government* (pp. 512-543). Oxford: Oxford University Press.

MOORE, A. D. (2000). "Employee Monitoring and Computer Technology: Evaluative Surveillance v. Privacy", *Business Ethics Quarterly*, Vol. 10, No. 3, pp. 697-709.

MORIARTY, J. (2005). "On the Relevance of Political Philosophy to Business Ethics", *Business Ethics Quarterly*, Vol. 15, No.3, pp. 455-473.

NAGEL, T. (1995). "Personal Rights and Public Space", *Philosophy and Public Affairs*, Vol. 24, No.2, pp. 83-107.

NEWELL, P. (2002). "Managing Multinationals: The Governance of Investment for the Environment", *Journal of International Development*, 13, pp. 907-919.

PESLAK, A. R. (2005). "An Ethical Exploration of Privacy and Radio Frequency Identification", *Journal of Business Ethics*, Vol. 59, No. 4, pp. 327-345.

RICHARDS, N. M. (2015). "Four Privacy Myths", in SARAT, A. (ed), *A World Without Privacy. What Law Can and Should Do? New York*, Cambridge University Press.

ROSENBERG, R. S. (1999). "The Workplace on the Verge of the 21st Century", *Journal of Business Ethics*, Vol. 22, No. 1, Ethics of Information and Communication Technology, pp. 3-14.

SCANLON, T. M. (2004). "Adjusting Rights and Balancing Values", *Fordham Law Review*, 72, pp. 1.477-1.486.

SEN, A. (1993). "Does Business Ethics Make Economic Sense?", *Business Ethics Quarterly*, Vol. No. 31, pp. 45-54.

SMITH, J. D., (2009). "Internet Content Providers and Complicity in Human Rights Abuse", in ARNOLD, D. G., BEAUCHAMP, T. L., BOWIE, N. (eds), *Ethical Theory and Business*. London: Prentice Hall International, pp. 442-445.

SOLOVE, D. J. (2002). Conceptualizing Privacy, *California Law Review*, Vol. 90, No. 4, pp. 1.087-1.155.

SOLOVE, D. J. (2011). *Nothing to Hide. The False Tradeoff between Privacy and Security*, New Haven- London: Yale University Press.

SPINELLO, R. A. (2010). "Informational Privacy", in BRENKERT, G. G. and BEAUCHAMP, T. L. (eds), *The Oxford Handbook of Business Ethics*, Oxford: Oxford University Press, pp. 366-387.

THOMSON, J. J. (1984). "The right to privacy", in SCHOEMAN, F. D. (ed.), *Philosophical Dimension of Privacy. An anthology*. New York: Cambridge University Press.

TINCANI, P. (2016). "Un altro dono dello spirito maligno. Nuova sorveglianza e comportamenti individuali", in PELLICCIOLI, L. (a cura di), *La privacy nell'età dell'informazione*, L'Ornitorinco, Milano.

WARREN, S. and BRANDEIS, L. (1890). "The Right to Privacy", *Harvard Law Review*, 4, pp. 193-220.

WHITMAN, J. Q. (2004). "The Two Western Cultures of Privacy: Dignity Versus Liberty", *Yale Law Journal*, 113, pp. 1.151-1.221.

ZICCARDI, G. (2016). *L'odio on line. Violenza verbale e ossessioni in rete*. Raffaello Cortina, Milano.

ZUCCA, L. (2007). *Constitutional Dilemmas*. Oxford: Oxford University Press.

## CASE LAW

Corte di Cassazione, III sez. pen., 3 Febbraio 2014, n. 3672.

Court of Justice in Case C-131/12.

Tribunal of Milan, 12 April 2010 n. 1972.

Corte di Appello of Milan, December 21, 2012.

## LEGISLATION

Art. 167 of Legislative Decree n. 196 of the 2003 Privacy Code.

## SITES

BARBER, L. and PALMER, M. (2010). "Google chief prizes creativity", June 3, 2010, https://on.ft.com/2ZSgJcx.

DONADIO, R. (2010). "Larger Threat Is Seen in Google Case, New York Times", https://nyti.ms/2P2FeTp.

EDWARDS, L. (2010). "Annoyed Now: Google & Italy, Pangloss", February 25, https://bit.ly/2OK6Dcl.

GILIOLI, A. (2010). "Piovono Rane", https://bit.ly/2YSjhpI.

GOOGLEBLOG (2010). Serious Threat to the Web in Italy, February 24, 2010, https://bit.ly/31tMloS.

GUARDIAN (2010). Google Street View "broke Australia's privacy law", https://bit.ly/2YzNHSm.

KAFKA, P. (2010). Google's European Road Trip Gets Even Worse, All Things Digital, February 24, https://bit.ly/2GTNaj4.

MUCCHETTI, M. (2010). "Il pm, la privacy e Google: loro vogliono il Far West", June 6, 2010, https://bit.ly/2ZfdgIF.

Repubblica (2010). Disabile picchiato e filmato, condannata Google. Gli Usa: "La libertà di internet è vitale", https://bit.ly/2KyxGC3.

Sole24 (2010). Minacciato su Facebook per la sentenza Google, April 15, 2010, https://bit.ly/2MNd5wI.

WARBURTON, D. (2010). "Google Moves China Operations to Hong Kong", March 23, 2010, ittps://bit.ly/2GTyRv6.

WHITCOMB, D. (2010). "Cyber-bullying Cases Put Heat on Google, Facebook", March 9, 2010, https://reut.rs/33mn9mc.

***Gianluca Andresani***
Researcher in the School of Law, Durham University, UK. Research Associate and former Director of the Professional and Institutional Ethics Programme, Institute of Applied Ethics, Hull. *E-mail*: gianluca.andresani@durham.ac.uk

***Natalina Stamile***
Associate lecturer of Philosophy and Legal Informatics at the University of Bergamo, Italy. Ph.D in Legal Theory and European Legal Order, Magna Graecia University, Catanzaro, Italy; post-doctorate in the Postgraduate Program in Law at the Federal University of Paraná, Brazil. *E-mail*: natalinastamile@yahoo.it