CREATe

CREATe Working Paper 2013/6 (May 2013)

# Twitter (R)evolution:

# Privacy, Free Speech and Disclosure

Authors

Lilian Edwards
University of Strathclyde
lilian.edwards@strath.ac.uk

Andrea Matwyshyn
University of Pennsylvania
amatwysh@wharton.upenn.edu

This paper will be presented at the International World Wide Web Conference, May 13–17, 2013, Rio de Janeiro, Brazil, and published in the WWW 2013 Companion (ACM 978-1-4503-2038-2/13/05).


CREATe Working Paper Series DOI: 10.5281/zenodo.8376.

This release was supported by the RCUK funded *Centre for Copyright and New Business Models in the Creative Economy (CREATe)*, AHRC Grant Number AH/K000179/1.

**ABSTRACT**
Using Twitter as a case study, this paper sets forth the legal tensions faced by social networks that seek to defend privacy interests of users. Recent EC and UN initiatives have begun to suggest an increased role for corporations as protectors of human rights. But, as yet, binding rather than voluntary obligations of this kind under international human rights law seem either non-existent or highly conflicted, and structural limitations to such a shift may currently exist under both US and UK law. Companies do not face decisions regarding disclosure in a vacuum, rather they face them constrained by existing obligations under (sometimes conflicting) legal demands. Yet, companies such as Twitter are well positioned to be advocates for consumers' interests in these legal debates. Using several recent corporate disclosure decisions regarding user identity as illustration, this paper places questions of privacy, free speech and disclosure in broader legal context. More scholarship is needed on the mechanics of how online intermediaries, especially social media, manage their position as crucial speech platforms in democratic as well as less democratic regimes.

**Categories and Subject Descriptors**
Security - *pseudonymity, anonymity and untraceability;* Human centered computing – *social networks, privacy.*

**General Terms**
Standardization, Security, Human Factors, Legal Aspects.

**Keywords**
Social networks, Twitter, pseudonymity, anonymity, privacy

## 1. Introduction

Much legal and policy work on global Internet censorship, such as *Access Denied* and associated Open Net Initiative surveys [1], has focused, understandably, on state interventions, especially in non-Western or non-democratic countries. Such work has recently highlighted not only established censorship regimes such as the Great Firewall of China but also *ad hoc* crackdowns such as the Internet shutdowns exerted or threatened during the "Arab Spring" of 2011. Increasingly though, state restrictions also work less obviously than in these high profile cases, through indirect influence, legal and extra-legal, on the *private* online intermediaries- companies such as ISPs, hosts, social networks, and telecoms companies – who most proximately control access to digital content. Such restrictions notably operate to functionally limit freedom of speech not only in non-democratic countries but also those generally considered more respectful of human rights and with strong free speech cultures such as those of the United States and United Kingdom.[1]

An interesting recent case study with which to examine "privatized censorship" in global social media context can be seen in the behavior of Twitter, the micro-blogging site associated strongly with the dissident internet activity during the Arab Spring. Twitter's recent decisions to publish a take-down policy [2] and guidelines for law enforcement with respect to information requests can be regarded as the best way forward for striking a balance between managing legal risk and preserving rights to free speech. However, critics may consider it to be a "sell out" [3] by one of the most open and rights-conscious of the major social networks, which previously described itself as "the free speech wing of the free speech party." [4]

In the UK, the actions of Twitter have special resonance, following as they do hard upon a period of riots in summer 2011, which were sparked by the shooting of a youth, Mark Duggan, by a police constable in Tottenham, but were also closely linked to prevalent unrest

[1] For additional information the Chilling Effects Clearinghouse website is useful and may be accessed at http://www.chillingeffects.org/.

among youth related to the anti-cuts movement and austerity measures. Social media were used as a locus for surveillance without warrant of suspected or potentially criminal or dissident behaviour, and at least one telecoms network (Blackberry/RIM) indicated that they were willing to disclose personal data about subscribers to the police on a voluntary not legally compelled basis.[2] Remarkably, threats were also made by Prime Minister David Cameron that social networks might be temporarily closed down by government fiat to prevent unrest. [5] In the US, the role of private intermediaries in content censorship and government information sharing has also been highlighted by the travails of Wikileaks [6] as well as recent subpoenas in connection with disclosing identities of users associated with the Occupy Wall Street Movement.

Given this complex and troubled background, more work is clearly needed on the mechanics of how online intermediaries, especially social media, manage their position as crucial speech platforms in democratic as well as less democratic regimes. Recent EC [7] and UN [8] initiatives have begun to suggest an increased role for corporations as protectors of human rights, but, as yet, binding rather than voluntary obligations of this kind under international human rights law seem either non-existent or highly conflicted (as in the jurisprudence of the ECHR and "horizontal effect", and the literature on corporate social responsibility). Voluntary online industry codes specifically designed to support free speech are also at an emergent stage, such as the Global Network Initiative, which includes Google, Microsoft and many NGOs and research centres. It would be fair to say these initiatives by no means embrace all the major players on the global digital content stage, and the future balance among privacy, free speech and disclosure remains uncertain.

## 2. Twitter – the United Kingdom experience

As noted above, Twitter, the micro-blogging site, has both attracted and fostered a reputation as one of the most free speech conscious social networks. Twitter's (and general social media) contribution to the Arab Spring uprisings, referred to above, has been contested but has undeniably etched itself into the global public consciousness. There is evidence that Facebook and YouTube were also used extensively by dissident parties.[3]

In the UK, Twitter attracted attention in particular as a beacon of free speech among social media sites during the "super-injunctions" fracas of May 2011. Twitter was the main locus for public defiance of so-called "super-injunctions" issued by the English courts in response to actions for breach of confidence/privacy by celebrity plaintiffs in 2011-12. In English common law, injunctions can reasonably easily be got to head off release of private details about public figures where there is no apparent public interest, in sharp contrast to traditional approaches in the United States, which traditionally abhor prior restraints and err on the side of allowing speech, even if actions for damages may follow subsequently. Invariably, UK privacy injunctions, where reported, anonymize the plaintiffs otherwise further privacy breaches would occur, eg the notorious case (see below) of Ryan Giggs, the England footballer, who sought to prevent publication of an alleged affair with a Big Brother contestant, the injunction in his favour being known *sub nom CTB v. News Group Newspapers* [2011] EWHC 1232 (QB). "Super-injunctions" go one step further, in that they forbid any reporting of the injunction even under anonymised form, and even communications with one's MP concerning the case. Greenslade [9] reports that in 2012, the number of public figures using privacy

[2] A helpful summary of these events may be found at http://www.guardian.co.uk/uk/london-riots.

[3] A further discussion of where Facebook, YouTube and texts via cell phones are mentioned equally as much as Twitter in the case studies of Egypt, Tunisia, Libya and others may be found at http://socialcapital.wordpress.com/2011/01/26/twitter-facebook-and-youtubes-role-in-tunisia-uprising/. The West as much abetted dictatorship by supplying censorware and surveillance technologies, as defied it via social media access.

arguments to protect their identity in England and Wales court actions rose to 24 from nine in 2010 (and just two in 2009). The Guardian published a fairly full list of anonymized celebrity privacy actions from 2007 to end 2011 – though not those covered by "super-injunctions", for the reason just described – and came up with 41 actions initiated, some unsuccessful. [10] The public reaction was however many times more voluminous than these figures would suggest. Public outrage at what was popularly seen as gagging of the press to protect celebrities trying to hide sexual misdemeanours by legal finagling came to a head with the Ryan Giggs case in May 2011. Although Giggs was successful in obtaining an anonymized (not "super") injunction, word rapidly spread on Twitter of the true identity of the plaintiff, and the revelations "went viral." [11] An account specially set up to reveal names of redacted plaintiffs gained about 100,000 followers. Confusion was added by the realisation that injunctions of the English courts did not run in nearby Scotland, after which the *Sunday Herald*, a Scottish broadsheet, became the first UK hard copy media to risk printing Giggs's name. [12] Shortly thereafter the matter descended into farce as essentially everyone in the UK who cared to know the name in question, but English media were still enjoined not to publish it. The matter was finally put to rest when an MP was persuaded to name the plaintiff in Parliament, protected as he was against contempt of court by Parliamentary privilege.

The germane point for this paper is that throughout this affair, Twitter apparently made no attempts to obey the by now well-known injunction protecting Giggs's privacy by blocking or removing tweets on the matter (even though hashtags might have made this relatively simple to automate), or suspending users who spread the meme. This persisted even when Giggs reportedly raised an action against Twitter for breach of injunction, even though chances of success were assumed to be low given Twitter's central establishment in the US outside the jurisdiction of English injunctions. [13] During this period Twitter said rather obliquely that it "strive[s] not to remove tweets on the basis of their content" but that it would remove "illegal tweets and spam." In January 2012, Twitter further noted that "to date Twitter has never received a super-injunction from the British courts." Twitter also asserted at the time that they would not disclose names of subscribers using pseudonyms without court order and without notifying that user first. Alexander Macgillvray, chief counsel, said on Twitter: "Our policy is notify users & we have fought to ensure user rights." [14] While privacy advocates were dismayed, Twitter's actions were seen by many as strongly anti-censorship, in stark contrast to how, for example, Amazon Web Services had dealt with Wikileaks. [15]

In January 2012, Twitter issued for the first time a formal statement of intent to systematically take down tweets on lawful request but with certain caveats to protect free speech. "*Starting today, we give ourselves the ability to reactively withhold content from users in a specific country — while keeping it available in the rest of the world. We have also built in a way to communicate transparently to users when content is withheld, and why [n 3 above].*" Twitter clarified that although they had yet to use this power, they could in the future block access to tweets which broke the law of country A to residents of country A only, thus not restricting speech elsewhere. This "granular" approach was also espoused by Google in February 2012. [16]

Twitter has so far put the new policy into operation twice in the EU. In October 2012, Twitter agreed to block the account of the Besseres Hannover group, a neo-Nazi group banned under German law. Similarly, in January 2013, Twitter agreed to remove certain trending anti-Semitic hashtags in France, such as #unbonjuif, and also deleted some related tweets from October 2012. So far, though, they have refused to identify the authors of the tweets for prosecution in France, pleading the First Amendment and their US base, despite being ordered

to do so by the French courts on January 24 2013.[4] [17] How far Twitter will fight to maintain a non disclosure policy, will be interesting given the pressures placed on them to disclose IDs to government and prosecutors discussed in **3** below.

Significantly, Twitter has also considered the transparency and notice aspects of their new policy. Any take downs are to be communicated via the Chilling Effects Clearinghouse (a model pioneered by Google). Even in country A, users will still see a "Tweet blocked" notice. Also following in the wake of Google, Twitter launched a Transparency Report in July 2012. [18] The report discloses government requests received for user information; government requests received to withhold content, and DMCA takedown notices received from copyright holders. In 2012, Twitter revealed they had received 48 non-DMCA related take down requests and 1850 disclosure requests in total. Interestingly, of these very few non-copyright take down requests, the only ones which had been actioned by Twitter in 2012 came from France (1, removed) and Germany (2, only 50% removed).

Finally and perhaps most interestingly, Twitter added a guide describing how the company would know what countries Twitter users lived in for blocking purposes. Although IP address might be used to identify users' locations, this identification could be "trumped" by explicit registration, which included the option "Worldwide": anyone choosing this option would thus see all tweets unrestricted by national censorship. [19] This "contractarian" self-disclosure approach to free speech leads us to consideration of the United States legal context, where free speech exists in an uneasy relationship with contract law.

## 3. Twitter - the Unites States experience

Anonymous and pseudonymous speech questions are embedded in a stronger regime of Constitutional speech protection in the United States than in the UK, but the primary law controlling questions of Twitter censorship and information disclosures is not actually the law of free speech – it is the law of contract. Although Justice Sotomayor's concurrence in *US v. Jones* recently questioned whether "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," [20] contract law is currently a potent circumvention tool for any free speech protection under the First Amendment with respect to private parties. The Twitter user agreement, therefore, forms the dispositive starting point for any privacy inquiry under US law. In other words, the permissibility of censorship of any particular user's speech or the sharing of information about that user with governmental authorities begins as a contract law question interpreting the Twitter user agreement.

Twitter's guidelines for law enforcement, state that: "Twitter's policy is to notify users of requests for their information prior to disclosure unless we are prohibited from doing so by statute or court order." In this vein, Twitter spokesperson Matt Graves has commented, "We can't comment on any specific order or request…However, to help users protect their rights, it is our policy to notify our users about law enforcement and governmental requests for their information, unless we are prevented by law from doing so." [21]

A series of recent subpoenas in connection with the Occupy Wall Street Movement have tested Twitter's commitment to this approach. In one case, the Suffolk Massachusetts District Attorney attempted to subpoena the tweets and user information of a user going by the handle @poisAnoN and listing and the name of Guido Fawkes. Although the Suffolk District Attorney requested that the subpoena remain secret in order "to protect the confidentiality and integrity of the ongoing criminal action," [22] Twitter nevertheless informed the user in question that

---

[4] A private group, the Union of Jewish French Students, is also suing Twitter in a Paris court for failing to obey the court ruling to identify users. Additional information regarding the case may be found at http://www.huffingtonpost.co.uk/2013/03/22/twitter-unbonjuif-anti-semitic-sued_n_2931990.html.

the District Attorney had subpoenaed the user's information. As a result, the ACLU of Massachusetts challenged both the subpoena and the secrecy of various court proceedings around the subpoena on behalf of the user in question. However, the Superior Court found that the ACLU and its client lacked standing to challenge the administrative subpoena, and the court ordered the documents to be produced. [23] The Assistant District Attorney allegedly argued that the user gave up his right to anonymity online when he joined Twitter, and that the "voluntary nature of the tweeting" is what "puts his IP address out there." [24]

Meanwhile, in connection with the Occupy Wall Street movement in New York, a writer named Malcolm Harris who was arrested for disorderly conduct recently challenged a subpoena from the Manhattan District Attorney's office to Twitter. The subpoena, issued to Twitter on January 26, 2012, demanded "any and all user information as well as any and all tweets posted for the period of 9/15/2011 – 12/31/2011" associated with @destructuremal, Harris's Twitter account. [25] Harris's attorney argued that the subpoena was overbroad, issued for an improper purpose and constituted an abuse of the court process; the request for "any and all information" could be interpreted as asking for private messages between Harris and others, as well other data collected by Twitter, including e-mail addresses and phone numbers used by Harris, websites he has visited and information about his physical location at different times. [26] However, the criminal court in Manhattan, much like the Manhattan court above, ruled that Harris lacked standing to oppose the subpoena delivered by prosecutors to Twitter. [27]

Even assuming that cases in connection with a pending criminal investigation may warrant allowing for additional prosecutorial discretion, Twitter also receives subpoenas that push the reasonable limits of law enforcement necessity. For example, Pennsylvania Attorney General Tom Corbett recently came under criticism in the press when he attempted to subpoena Twitter demanding the name, address, contact information, creation date, creation IP address, and any and all log in Internet protocol address of two anonymous critics who were using Twitter to criticize him. [28] Although the subpoena was ultimately dropped, it demonstrates the tension between governmental attempts to obtain privately held information and the privacy interests of users. These tensions will continue to heighten. Particularly if courts continue to deem users to lack standing to challenge Twitter subpoenas, this leaves Twitter in a somewhat untenable public relations position, despite trying to offer users the ability to quash inappropriate subpoenas: Twitter may be the only party deemed to have standing to move to quash.

Twitter has, arguably, to this point been at the forefront of transparency (see discussion in **2** above), however this decision of whether to step into court to defend privacy interests of users will undoubtedly be a carefully pondered business decision. While some stakeholders may argue that it is not Twitter's place to take a firm position defending privacy of users because of a potentially detrimental impact on short-term shareholder value, other stakeholders might disagree. They might point to the state level corporate constituency statutes in the United States, which expressly empower officers and directors of companies to consider interests of all impacted stakeholders in the enterprise in decision-making, not merely short-term financial interest of shareholders. Twitter users would certainly form one type of impacted stakeholder group. Should Twitter choose to become the social network known for its firm pro-user privacy positions and cooperate with users to quash subpoenas, this stance can easily be explained as a logical corporate decision intended toward maximization of long-term value for the company and consumer goodwill generation.

Meanwhile, for public companies in the US, arguably US securities laws may require disclosure of significant volumes of information requests and other corporate information disclosure behaviors. As a general rule, public companies are required to disclose any risks to future revenues which may have a "material adverse effect." One type of material adverse

effect may include a substantial loss of important customers.[5] In the case of a technology company whose primary business line involves interpersonal communications – Twitter, Google, Microsoft, Facebook etc. – if public, an argument can be made that failing to disclose a large volume of information sharing with government authorities is an act of withholding information that a reasonable shareholder would like to know in order to gauge his investment interest. We have seen consumers become enraged en masse over privacy policy changes that are disclosed; it is possible that consumers would be equally enraged over high volumes of information sharing with authorities, particularly if deemed surreptitious. If large numbers of users become disenchanted and discontinue use, it is possible that a reportable material shift in revenues will occur. Further, the Securities and Exchange Commission has begun to issue guidance with respect to information security and privacy disclosures, but corporate practices are still inconsistent with respect to disclosure. [29] Perhaps anticipating these securities law concerns, Google has constructed aggregated transparency reports [30] online where it provides statistics by country with respect to government agency and court removal information requests, albeit with at least a 6+ month delay in posting as of this writing and subject to certain limitations. [31] Google, as well as Microsoft, also recently began to disclose the receipt of National Security Letters. [32] However, Google has simultaneously faced criticism in the press for its willingness to comply with subpoenas without giving users a chance to quash. Critiques have noted that in light of Google's positioning itself as a protector of user rights, this failure to alert users to the existence of the subpoena creates an inconsistent impression. [33] As discussed above, Twitter faces similar challenges.

## 4. Discussion and implications

From a UK perspective, then, 2011 began with a fear of possibly widespread social media censorship, a fear which seemed fairly possible at the time of the super-injunction fracas and later during the 2011 summer riots. In this context, Twitter's new policies seem a clever attempt to balance two goals: one, avoiding legal risk as a publisher and two, supporting free speech (and the good will of pro-free speech users). The elements of granularity, transparency, notice, "rule of law" via a clear policy on what justifies take down [34], and especially the implied ability to evade the system by user preference, change the calculus. While it may be true on its face that Twitter is moving away from a radical free speech position, as a legal matter, Twitter has always contractually reserved the right to dictate the terms of its service, and still demonstrates a more pro-user position with respect to privacy than is the industry norm. Because of the standing problems identified above, the current process of notifying users of government subpoenas, while useful for transparency, may be futile from the standpoint of actually quashing an overreaching subpoena without more active participation from Twitter. This is particularly questionable given the evidence in Twitter's own Transparency Reports: according to them, in the first half of 2012, 679 requests for "user information" (including subpoenas) were made by the USA of which 75% were actioned, either wholly or partially. In the second half of 2012, the number of US requests rose to 815 and 69% were wholly or partially met. It has to be questioned also how far Twitter can maintain a doggedly pro privacy approach when disclosure of identities by platforms is relatively routine in many EU states where Twitter also operates, such as the UK[6] and France.

UK and US attitudes may also differ based on the underlying legal risks and liabilities of the respective systems. Free speech advocates would expect Twitter to be bold in what content

---

[5] Item 101, Regulation S-K is an example of such a Securities and Exchange Commission disclosure, requiring a corporation to disclose customers whose loss may impact ~10%+ of net revenue.

[6] In the UK, the opinion in *Totalise v. Motley Fool* [2001] EWCA Civ 1897 discussed when a court should require disclosure and when so asked, balance privacy interests against seeking justice. Prior to this case, it often seemed that disclosure was usually simply automatically required by courts on request.

it hosts and distributes, pointing out that online publishers usually have statutory immunity in respect of third party content they carry.[7] [35] On the other hand, in the EU and UK, online intermediaries become fully liable for all unlawful content they host or distribute on notice if they do not take down expediently. [36] Finally neither system really has yet found an answer, legally or ethically, to the thorny problem of what a private online intermediary should do faced with demands for censorship or disclosure by a government where no real democratic norm operates as to freedom of speech. Twitter, since the arrival of its new take down policy, has not yet grappled with what it would do if an authoritarian government like Egypt's pre-Arab Spring were to ask for suppression of speech, apparently backed by local law; Twitter did however indicate in the January 2012 blog post that: "*As we continue to grow internationally, we will enter countries that have different ideas about the contours of freedom of expression. Some differ so much from our ideas that we will not be able to exist there*". Twitter also guaranteed in the same post the principle of only *post hoc* take down, as opposed to prior filtering.

In conclusion, Twitter's future, given its very public profile as a locus for free speech will be a fascinating case study as it seeks to safeguard its corporate position as well as satisfy its global and various user constituencies. The clash of physical space jurisdictional demands and differing national legal contexts around privacy, free speech and disclosure have created irreconcilable tensions for companies trying to preserve user privacy and freedom of expression. Yet, companies such as Twitter are well-positioned to be advocates for consumers' interests in these ongoing legal debates. They can serve as defenders of user privacy and free speech against governments that seek to obtain progressively greater amounts of information about users, sometimes in ways that evade traditional procedural safeguards or violate principles of human rights.

## REFERENCES


1. *Home, Oni Access: Denied Controlled Contested*. 2011. URL: http://access.opennet.net/.
2. Twitter. *Tweets still must flow*. Jan. 2012. URL: http://blog.twitter.com/2012/01/tweets-still-must-flow.html .
3. Beschizza, Rob. *Twitter's early bird special on censorship*. Jan. 2012 URL: http://boingboing.net/2012/01/31/twitters-early-bird-special.html.
4. Halliday, Josh. *Twitter's Tony Wang: "We are the free speech wing of the free speech party*." Mar. 2012. URL: http://www.guardian.co.uk/media/2012/mar/22/twitter-tony-wang-free-speech . Twitter also published a blog explicitly espousing the human right to freedom of expression and resisting pressure to censor during the Arab Spring: http://blog.twitter.com/2011/01/tweets-must-flow.html.
5. Halliday, Josh. *David Cameron considers banning suspected rioters from social media*. Aug. 2011. URL: http://www.guardian.co.uk/media/2011/aug/11/david-cameron-rioters-social-media?INTCMP=ILCNETTXT3487 .
6. Edwards, Lilian. *Wikileaks, online intermediaries and privatised censorship*. URL: http://blogscript.blogspot.co.uk/2011/02/wikileaks-online-intermediaries-and.html.
7. European Commission. *Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions*. Oct. 2011. URL: http://ec.europa.eu/enterprise/policies/sustainable-business/files/csr/new-csr/act_en.pdf .


[7] The Communications Decency Act and the Digital Millennium Copyright Act each offer liability limitation to intermediaries.

8. Ruggie, John. *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*. Mar. 2011. URL: http://www.business-humanrights.org/media/documents/ruggie/ruggie-guiding-principles-21-mar-2011.pdf.
9. Greenslade, Roy. *Privacy Injunctions on the Rise*. Dec. 2011.URL: http://www.guardian.co.uk/media/greenslade/2011/dec/05/privacy-press-intrusion.
10. Butterworth, Siobhan. *Superinjunctions, Gagging Orders, and Injunctions: The Full List*. Aug. 2011. URL: http://www.guardian.co.uk/law/datablog/2011/aug/05/superinjunctions-gagging-orders-injunctions-list.
11. Halliday, Josh. *Ryan Giggs Helps Facebook, Twitter and LinkedIn to Record Month*. June 2011. URL: http://www.guardian.co.uk/technology/2011/jun/27/ryan-giggs-facebook-twitter-linkedin.
12. *Sunday Hearld Editor Defends Injunction Story*. May 2011. URL: http://www.thedrum.co.uk/news/2011/05/23/sunday-herald-editor-defends-injunction-story .
13. Halliday, Josh. *Twitter Faces Legal Action by Footballer Over Privacy*. May 2011. URL: http://www.guardian.co.uk/media/2011/may/20/twitter-sued-by-footballer-over-privacy?INTCMP=SRCH.
14. Halliday, Josh. *Twitter Will Notify Users Accused of Gagging Order Breaches.* May 2011. URL: http://www.guardian.co.uk/media/2011/may/25/twitter-privacy-injunction-battle?INTCMP=SRCH .
15. MacAskill, Ewen. *WikiLeaks Website Pulled by Amazon after US Political Pressure*. Dec. 2010. URL: http://www.guardian.co.uk/media/2010/dec/01/wikileaks-website-cables-servers-amazon.
16. Out-Law.com. *Google-hosted Blog Content to be Censored on Country-by-Country Basis*. Feb. 2012. URL: http://www.out-law.com/en/articles/2012/february/google-hosted-blog-content-to-be-censored-on-country-by-country-basis/.
17. Farr, Christina. *Twitter is Under Pressure to Identify the Racist Users Behind #unbonjuif*. Jan. 2013. URL: http://venturebeat.com/2013/01/24/twitter-is-under-pressure-to-identify-the-racist-users-behind-unbonjuif/.
18. Twitter.com. *Twitter Transparency Report*. July 2012. URL: http://blog.twitter.com/2012/07/twitter-transparency-report.html.
19. Twitter.com. *Changing Your Country Settings*. 2013. URL: https://support.twitter.com/articles/20169220#
20. *United States v. Jones*, 132 S. Ct. 945, 957 (2012).
21. Copeland, Dave. *Twitter Ignored Request to Keep Subpoena Under Wraps*. Dec. 2011. URL: http://www.readwriteweb.com/archives/twitter_ignored_request_to_keep_subpoena_under_wraps.php.
22. *Administrative Subpoena*. Dec. 2011. URL: http://privacysos.org/sites/all/files/OBtwittersubpoena.pdf.
23. American Civil Liberties Union. *ACLU of Massachusetts Makes Statement on Twitter Subpoena Case*. March 2012. URL: http://www.aclu.org/technology-and-liberty/aclu-massachusetts-makes-statement-twitter-subpoena-case.
24. Privacy SOS. *Online Denizens: The Government Says You are Better off Passing out Flyers in a Ski Mask than Tweeting Controversial Material*. Feb. 2012. URL: http://privacysos.org/node/475.
25. McVeigh, Karen. *Occupy Wall Street Protester Vows to Fight Subpoena over Twitter Account*. Feb. 2012. URL: http://www.guardian.co.uk/world/2012/feb/07/occupy-protester-subpoeana-twitter.

26. Coscarelli, Joe. *Occupy Wall Street Protester Laughing off Twitter Subpoena*. Feb. 2012. URL: http://nymag.com/daily/intel/2012/02/ows-protester-laughing-off-twitter-subpoena.html.
27. Moynihan, Colin. *Judge Rules that Protester Can't Oppose Twitter Subpoena*. April 2012. URL: http://cityroom.blogs.nytimes.com/2012/04/24/judge-rules-that-protester-cant-oppose-twitter-subpoena/.
28. Masnick, Mike. *Pennsylvania AG Tom Corbett Can't Take Anonymous Twitter Criticism; Issues Supoenas for IDs*. May 2010. URL: http://www.techdirt.com/articles/20100519/1031479492.shtml
29. Reuters. *Disclosures 2012: Level of Cyber-Security Risk Disclosures Varies After New SEC Guidance*. April 2012. URL: http://blogs.reuters.com/financial-regulatory-forum/2012/04/06/disclosures-2012-level-of-cyber-security-risk-disclosures-varies-after-new-sec-guidance/.
30. Google. *Transparency Report*. 2013. URL: http://www.google.com/transparencyreport/governmentrequests/map/.
31. Google. *Transparency Report: FAQ*. 2013. URL: http://www.google.com/transparencyreport/faq/#governmentrequestsfaq.
32. Kravets, David. Microsoft, Too, Says FBI Secretly Surveilling Its Customers. March 2013. URL: http://www.wired.com/threatlevel/2013/03/microsoft-nsl-revelation/
33. Masnick, Mike. *How Far Should Google Go To Protect User Privacy in Lawsuits?* Aug. 2009. URL: http://www.techdirt.com/articles/20090831/1713366058.shtml
34. Twitter. *Country Withheld Content*. 2013. URL: https://support.twitter.com/articles/20169222#.
35. 47 USC. § 230 (1996).
36. Council and Parliament Directive 2000/31/EC, arts. 12-15, O.J. SPEC. ED.

RCUK Centre for Copyright and
New Business Models in the
Creative Economy

College of Social Sciences / School of Law
University of Glasgow
10 The Square
Glasgow G12 8QQ
Web: www.create.ac.uk