Twitter and other blogs, Facebook, emails, SMS messages, LinkedIn, Youtube and Flickr are ubiquitous forms of communication within modern society. The role of these tools in enabling individuals to express their political opinions, as well as whether and how social media should be regulated, have emerged as questions of considerable interest. However, the issue of locating social media within a possible conflict between regulation and democracy remains underexplored. Law is just one of the forces or ‘regulators’ that control and define systems such as the internet, the others being markets, architectures and norms.\(^2\) Civil or political liberties within cyberspace will only be enhanced if these forces are democratic in nature.\(^3\)

This chapter will assess two broad propositions: first, that social media has the potential to enhance democratic participation, and secondly, that legal restrictions can curtail this opportunity. These topics are significant because the influence of social media is frequently overstated and, in debates where democracy is at stake, the desirability of regulatory controls is typically overlooked. Part one defines social media and explores the premise that social media is conducive to enhanced democracy. It also identifies some of the risks and dangers of relying on this particular medium as a means of political participation. Part two will illustrate sources of and solutions to contests between law and democracy by reference to the human right to freedom of expression. Permissible limitations and restrictions on the exercise of that right can be identified from the paradigm of international human rights law. Those considerations will inform an analysis of a posited conflict between law and democracy. Particular attention is given to recent developments within the United States, Europe, China, and Australia. There is an observable trend towards greater government regulation of social media within each of these jurisdictions for national security, law enforcement and other reasons. Underlying themes to be addressed include notions of individual liberty, conditions of access to and participation in social media, the permissibility of restrictions within a democratic society, sound regulatory

\(^1\) srtully@gmail.com.

\(^2\) Lawrence Lessig, Code and Other Laws of Cyberspace (Basic Books, 1999).

development and ensuring government accountability. I contend that, in order to accommodate competing policy priorities, the adoption of regulatory measures inevitably but necessarily impairs the enjoyment of human rights and constrains the civic potential offered by social media.

**Social media as a means of political participation**

Social media may be defined as a group of internet-based applications which build on the ideological and technical foundations of Web 2.0, and allow the creation and exchange of user-generated content. Social networking sites such as Facebook provide an online presence for users to share information, search for others and communicate. Blogs such as Twitter enable users to publish commentary and broadcast it publicly over the internet. Social media such as YouTube enables users to publish and share images, videos and music through the internet. Whatever the particular form, social media has several common characteristics. First, a capability to attract a wide audience. Second, content is created when one user communicates with another.

Social media is fast becoming the preferred mode for education, employment, commerce and personal expression. Indeed, non-access and disconnection from the internet has been described as tantamount to ‘non-existence’. Social media may be employed for a range of purposes. For example, the capacity for social media to provide accurate and timely information makes it a useful tool for promoting human rights. During the Kosovo conflict, for example, NATO states targeted Serb media outlets conveying government propaganda but not internet service providers. It was considered that ‘full and open access to the Internet can only help the Serbian people know the ugly truth about the atrocities and

---


5 Content is ‘user generated’ if it is available to a select group on a publicly-accessible website or a social networking site, entails a minimum amount of creative effort, and is created outside of professional routines and practices: Organisation for Economic Cooperation and Development, *Participative Web and User-Created Content: Web 2.0, Wikis and Social Networking* (2007) 18.


crimes against humanity being perpetrated in Kosovo by the Milosevic regime.\textsuperscript{8} Human rights non-governmental organisations benefit from the internet with respect to information dissemination and ease of communication.\textsuperscript{9}

The internet has also changed the social conditions of speech. The cultural and participatory features of the human right to freedom of expression are accentuated.\textsuperscript{10} The United Nations (UN) Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mr Frank La Rue, has been mandated to provide his views on the advantages and challenges of new information and communication technologies, including the internet and mobile technologies.\textsuperscript{11} He believes that the internet is ‘inherently democratic’ because it provides the public with access to information and enables individuals to actively participate in the process of communication.\textsuperscript{12} In his view, the internet facilitates citizen participation in building democratic societies.\textsuperscript{13} Marginalised or disadvantaged social sectors can also obtain information and participate in public debates concerning social, economic and political changes affecting their circumstances.\textsuperscript{14}

But the relationship between social media and political participation is not so unequivocal. One view is that social media is the catalyst for political transformation — information is so widely accessible that individuals can formulate and express their own political opinions.\textsuperscript{15} On this account, social media fosters popular participation and greater democratisation within states. Through the internet, ‘[i]ndividuals become less passive, and thus more engaged observers of social spaces that could potentially become subjects for political conversation; they become more engaged participants in the debates about their observations’.\textsuperscript{16} Nevertheless, commentators are divided between those considering the internet to be a boon to democracy\textsuperscript{17} and those believing it is a tool of oppression.\textsuperscript{18}

\textsuperscript{11} Human Rights Council, Resolution 7/36 (2008) [4(f)].
\textsuperscript{13} Frank La Rue, Special Rapporteur, Report on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/17/27 (16 May 2011) [2], [19].
\textsuperscript{14} ibid [62].
It is admittedly true that the internet can prove to be an effective mechanism for political activism, particularly when combined with traditional forms of communications media. Social media facilitates activities as diverse as public education, fundraising, forming coalitions across geographical boundaries, distributing petitions or action alerts, and planning or coordinating events on a national, regional or international level. The internet and email, for example, has helped to organise consumer boycotts against multinational corporations and assist campaigns such as the adoption of selective purchasing legislation in Massachusetts against Myanmar.

The role of social media during the so-called ‘Arab Spring’ has also attracted considerable comment. In Egypt, for example, various groups used social media platforms, including Facebook and Twitter, to spread revolutionary messages and coordinate protests. Blogging became a source of information for political activists free from censorship or manipulation by the traditional state-controlled media. The government identified Facebook as a harmful application and officials joined Facebook groups to warn individuals not to strike. Mobile phones were banned in police stations to prevent the recording of YouTube videos.

Then, on 28 January 2011, then President Hosni Mubarak disconnected the internet for five days across the entire state. US President Obama indicated support for the right of Egyptians to the freedom of speech and to access information, observing that ‘we’ve seen the incredible potential for technology to empower citizens and the dignity of those who stand up for a better future’. US Secretary of State Clinton urged the Egyptian authorities ‘not to prevent peaceful protests or block communications, including on social media sites’. However, encouraging social media use as a means of facilitating human rights and a transition to a democratic political system runs up against the international

---

legal norm prohibiting intervention within the internal affairs of a state. Nevertheless, following 18 days of protest, Mubarak resigned from office and so ended 30 years of authoritarian rule.

Social media has had a comparable role in events within other states. In Tunisia, for example, videos of protests were uploaded to Facebook. In 2001, written accounts, photographs, videos and other information from Syrian demonstrators were relayed around the world via social media by 20 Syrian exiles. But social media can also be used to coordinate destructive mayhem within democratic states as much as effect constructive political mobilisation within authoritarian ones. Blackberry’s encrypted messenger service, for example, was blamed by UK Prime Minister David Cameron for coordinating British riots in August 2011.

Twitter on the other hand was credited with organising cleanups.

The contrary view is that social media promotes weak political ties and low-risk activism (or ‘slacktivism’) because ‘liking’ something on Facebook, or retweeting a story, takes little effort but lulls protagonists into believing that they are acting meaningfully. The vast quantity of information available through the internet can readily distract individuals from important political issues.

It has also been suggested that the level of internet connectivity can predict the degree of democratic attainment. In other words, the more enhanced the basic communications infrastructure of any given country then the more likely this will be conducive to the assertion and manifestation of liberties and rights for its citizens. The important civic value of the internet is that ‘those who have computers and internet communications find themselves better trained, better informed, and better able to participate in democracy’. Internet usage was a more accurate predictor of democracy between 2001–2002 than 1992–2002, thereby suggesting that the internet has only recently come into its own as a positive force for democratisation.

The experience of web-enabled open government illustrates the nature of individual behaviour and the challenges confronting agencies. The internet is opening up government agency methodologies to public scrutiny, prompting...
greater transparency, making information more accessible and increasing public participation in agency decision-making. For example, ‘e-rulemaking’ allows public comments to be submitted online through social media to formulate rules. However, individuals are exhibiting ‘drive-by participation’. Public participation can moreover delay agency action, overwhelm decision-makers and encourage agendas which meet the wishes of small, but vocal, interest groups. Thus the law and Web 2.0 become ‘very strange bedfellows. Law is authoritarian, hierarchical, and bounded; the Web is fluid, infinitely possibilistic, even anarchic.’

One difficulty with social media is that participation is characterised by inequality. There is intense participation by a small proportion of users who supply a large percentage of content. Ideally, individuals can collect factual information, voice their personal perspective, confront other points of view and rationally discuss issues. However, the internet is also a powerful tool for spreading misinformation, propaganda and hateful messages. Drawing the line between robust debate which advances knowledge-creation and speech that harms civic deliberations is therefore challenging. Can these dangers and risks be adequately addressed by regulation?

The second difficulty is that, while the number of internet users has increased exponentially, the internet’s growth and corresponding benefits are unequally distributed. Is it satisfactory, then, that the opportunity for political participation is left to depend upon such rudimentary issues as technology, infrastructure or electricity access? The problem of relying upon the internet as a democratising tool is that there is no universal access. The ‘digital divide’ refers to the unequal distribution of information and communication technology between and within states. In contrast to the 71.6 internet users per 100 inhabitants within developed states, there are only 21.1 internet users per 100 inhabitants in developing ones.

---

35 ibid 453.
and only 9.6 users per 100 inhabitants within Africa. Digital divides also exist within states along wealth, gender, geographical and social lines. Internet access tends to be concentrated among socioeconomic elites, whereas individuals in rural areas confront obstacles including lack of technological availability, slower connection speeds and/or higher costs. Disadvantaged sectors, such as disabled persons or minority groups, often face barriers to accessing the internet in a way that is meaningful, relevant and useful to their daily lives.

The international community is only beginning to address these challenges. For example, the World Summit on the Information Society defined the digital divide in access-related statistics. However, physical access — namely, possessing computers, user numbers, connection speeds and the underlying infrastructure — is only one dimension. By focusing upon access or enabling infrastructure, the question is posed: ‘how do we increase the speed of connections?’ This question should be reframed as how to encourage local communities to meaningfully participate. Meaningful participation, however, may have to overcome yet another hurdle: regulation by governments.

Government regulation of social media as a democratic impediment

The leading developed states agree that the internet helps to promote democracy and the freedoms of opinion, expression, information, assembly and association. Arbitrary or indiscriminate censorship or restrictions on internet access are said to be inconsistent with a state’s international obligations and are unacceptable. They have accordingly committed themselves to encouraging internet use as a tool for advancing human rights and democratic participation. Importantly, however, implementing these objectives is qualified by respect for the rule of law. Furthermore, as will be considered below, the promotion of social media use by governments has a Janus-like quality which reins in trends towards greater democratic participation.

---

39 International Telecommunication Union, Key Global Telecom Indicators for the World Telecommunication Service Sector, 21 October 2010.
43 ibid [11], [13], Section II [10].
It is clear from the previous discussion that the internet has a growing significance for the individual rights to freedom of opinion, expression and association as defined under international human rights law. The right to freedom of expression, for example, can illustrate the conflict between law and democracy in the context of social media. This right includes the freedom to seek, receive and impart information and ideas of all kinds, irrespective of frontiers, through any media of an individual’s choosing.

More particularly, a direct link between freedom of expression through social media and political participation can be identified. The free exchange of information or ideas on matters relevant to the economic, social or political life of a state is crucial to, and inherent in the very nature of, a democratic country. Freedom of expression including political debate is an essential foundation for a democratic society and a basic condition for individual self-fulfilment. Freedom of expression, together with the right to take part in the public affairs of a state, ‘implies that citizens, in particular through the media, should have wide access to information and the opportunity to disseminate information and opinions about the activities of elected bodies and their members’. The UN Human Rights Committee has already made the point that excluding individuals from accessing the Press Gallery for reasons of parliamentary privilege, for example, violated the right to freedom of expression ‘[i]n view of the importance of access to information about the democratic process’, notwithstanding the ability to report on proceedings through broadcasting services.

So, what then is the nature of this conflict between law and democracy? The first part of this chapter indicated that the individual interest in free political expression does not always coincide — and indeed may clash — with governmental agendas. The appeal of an unhindered multimedia communication space appears at odds with exercising control in the broader public interest. What role if any does law have in either bridging or perpetuating that gulf?

---


46 Campbell v MGN Limited [2004] UKHL 22, [148]–[149] (Baroness Hale).

47 Lingens v Austria [1986] 8 ECHR 407, [41]–[42].


49 ibid [13.5].
First, the law provides boundaries on the measures which states are permitted to adopt. Using the right to freedom of expression to illustrate the point, any limitations on this right must satisfy a three-part, cumulative test:50

a) the limitation must be provided by law which is clear and accessible to everyone (that is, the principles of predictability and transparency);

b) the limitation must protect the rights or reputations of others, national security, public order, public health or morals51 (the principle of legitimacy); and

c) the limitation must be necessary and the least restrictive means for achieving the purported aim (the principles of necessity and proportionality).

In addition, any legislative measure must be applied by a body which is independent of any political, commercial or other unwarranted influences in a manner that is neither arbitrary nor discriminatory, and having adequate safeguards against abuse, including the prospect of challenge and a remedy against any abusive application.52

International benchmarks such as these as a guide for national-level regulations are all well and good. But states are increasingly censoring online information by arbitrarily blocking or filtering content, criminalising legitimate expression, imposing intermediary liability,53 disconnecting users from internet access54 (for reasons including intellectual property rights protection)55 and inadequately protecting data privacy. For example, ‘timed’ blocking prevents users from accessing the websites of opposition parties or independent or social media at key political moments such as elections, times of social unrest, or political

---

51 International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entry into force 23 March 1976) art 19(3).
52 ibid [24].
53 ibid [39], [40]. See, for example, Law 5651 on the Prevention of Crime Committed in the Information Technology Domain 2007 (Turkey) grants authority to an administrative agency to issue orders to block websites for content hosted outside state borders. The Computer Crimes Act 2007 (Thailand) imposes liability upon intermediaries which transmit or host third-party content as well as the authors themselves. States have instituted ‘notice-and-takedown’ regimes which protect intermediaries from liability provided they promptly remove unlawful material upon notification. See, for example, Council Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market OJ L 178 (17 July 2000), 1–16, art 14; Digital Millennium Copyright Act of 1998, 112 Stat. 2860 (1998) s 512.
54 On a centralised ‘on/off’ control over Internet traffic, see ‘Reaching for the Kill Switch’, The Economist, 10 February 2011.
55 Legislation may disconnect users from the internet if they violate intellectual property rights, this occurring by way of a ‘graduated response’, that is, a series of increasing penalties which ultimately lead to suspending the internet service. See, for example, Conseil Constitutionnel, Decision 2009–580, Act furthering the diffusion and protection of creation on the Internet, 10 June 2010, http://www.conseil-constitutionnel.fr/conseilconstitutionnel/root/bank_mm/anglais/2009_580dc.pdf. See also Digital Economy Act 2010 (UK) ss 3–16.
or historically-significant anniversaries. States restrict, control, manipulate
or censor information disseminated through the internet either absent any
legal basis, using broad and ambiguous laws without justification or in an
unnecessary or disproportionate manner for achieving their intended aim. States
are moreover introducing or modifying laws to increase their ability to monitor
internet users’ activities as well as the content of communications without
sufficient guarantees against abuse. Government measures include a real-name
identification system before users can post comments or upload content (which
compromises anonymity) and restricting the use of encryption technology.\(^\text{56}\)

Such steps might not at first glance appear conducive to democratic ideals.
These regulatory measures are introduced for national security, counter-
terrorism or public order reasons such as protecting an individual’s reputation.
Indeed, international agreements may require states Parties to criminalise
certain activities committed over the internet.\(^\text{57}\) Content which may legitimately
be restricted includes child pornography, hate speech, defamation, direct and
public incitement to genocide, advocating national, racial or religious hatred
and incitement to discrimination, hostility or violence. These standards provide
permissible grounds for states to regulate contrary to an individual’s right to
freedom of expression. States are moreover supporting the growth of information
and communications technology to further their own specific ends including
national development objectives.\(^\text{58}\)

Within the international community China is frequently singled out for
criticism. The government is encouraging expansion of the internet and putting
more official information online.\(^\text{59}\) Because political discussion occurs on bulletin
boards and websites, the government has increased its efforts to monitor and
control content. Sophisticated and extensive filtering systems block access
to websites containing key terms such as ‘democracy’ and ‘human rights’.\(^\text{60}\)
Politically-sensitive websites including foreign news services are shut down by
authorities. Internet cafes are monitored or raided, and website operators are
jailed for subversion or social crimes. The authorities also monitor and block

\(^{56}\) Frank La Rue, Special Rapporteur, *Report on the Promotion and Protection of the Right to Freedom of
Opinion and Expression*, UN Doc A/HRC/17/27 (16 May 2011) [26], [30], [55].
\(^{57}\) *Convention on Cybercrime*, opened for signature 23 November 2001 (2001) ETS No 185 [entry into force 1
\(^{58}\) UN GA Res 55/2 on the Millennium Development Goals, UN Doc A/RES/55/2 (18 September 2000) Target
8f; World Summit on the Information Society, 2003 *Plan of Action*, WSIS-03/Geneva/DOC/5-E, Geneva, 12
Practices, China (including Hong Kong and Macau)*, 23 February 2001.
People You Might Know

television conversations, fax transmissions, email and internet communications. An email filtration system for anti-government messages entering China has also been established.

These measures of political repression are effected by law. The Measures for Managing Internet Content Provision, for example, regulate who can own an internet business and what is published online. Internet content providers must retain files of posted communications including details of who has read it for 60 days. Internet service providers must record the time that users log on to the internet as well as telephone and account numbers, internet addresses and domain names. State Council Order Number 273 (1999) requires firms with encryption technology to register and provide the names, telephone numbers and email addresses of all persons using it. These efforts to block content and control internet use, however, has only had limited success because sophisticated users can bypass such measures, the number of internet sites has grown so rapidly, censorship regulations are applied inconsistently and enforcement efforts vary. In sum, the contest between government control through regulation and democratic participation, like numerous other contexts within China, is being played out through the use of social media tools.

But one need not limit scrutiny to China to observe comparable steps taken by other states. Indeed, tighter regulatory control over social media is not limited to authoritarian states. For example, the European Union has developed more effective legislation to counter terrorist websites than the US because the right to freedom of speech is upheld with less vigour.61 European states must retain data generated or processed following a communication or use of a communication service.62 Internet service providers must retain user identification, telephone numbers and IP addresses for both the sender and recipient of communications.

Around 45 other states restrict internet access by their citizens, typically by forcing individuals to subscribe to state-run internet service providers which filter out objectionable material.63 The UN Human Rights Committee has also expressed concern that access to local and international sources of political commentary is blocked during election periods.64 Government surveillance of human rights defenders or political opposition figures communicating via the internet and Facebook can occur in an arbitrary or covert manner.

---

64 Human Rights Committee, General Comment No 34: Article 19: Freedoms of opinion and expression, UN Doc CCPR/C/GC/34 (12 September 2011) [37].
Non-governmental organisations in the human rights field are concerned that the threats to internet freedom are growing and becoming more diverse. In one study of 37 states, 15 blocked politically-relevant content. Reports of internet filtering, content manipulation and imprisoning users have increased in recent years. For example, in Brazil, India, Indonesia, South Korea, Turkey and the UK, internet freedom is increasingly undermined by legal harassment, opaque censorship laws or expanding surveillance. In Venezuela, Azerbaijan, Jordan and Rwanda, politically-motivated internet controls are emerging, typically during election periods. Increasing censorship and user arrests occurred in Bahrain, Ethiopia and Tunisia following popular protests or contentious elections. Following the 2009 elections, Iran established a filtering system which can block websites nationwide within several hours. In Vietnam, four activists were imprisoned for using the internet to express pro-democratic views. As is the case in China, however, resourceful citizens within these states continue to identify technical means with which to sidestep restrictions and employ internet-based platforms with a view to promoting greater participation.

The leading democratic states are by no means exceptional. Indeed, they have championed internet freedom for individuals located in other states — and to extend their governmental influence extraterritorially — whilst simultaneously introducing legislation which increases governmental surveillance and undermines the privacy of their own nationals. For example, the US promotes internet freedom and encourages universal access. In 2010, Secretary of State Clinton advocated ‘the freedom to connect — the idea that governments should not prevent people from connecting to the internet, to websites, or to each other’. The State Department supported new tools which enabled citizens to exercise their right to freedom of expression by circumventing politically-motivated censorship. It intends to put social media tools ‘in the hands of people who will use them to advance democracy and human rights’. However, the US is establishing links with foreign non-governmental actors with a view to furthering its own diplomatic objectives, including enhancing its ability to influence developments occurring within other states and skirt the norm of non-intervention in domestic affairs.

66 ibid 2–3.
67 See, for example, the Cyber Intelligence Sharing and Protection Act of 2012 (US); Cybersecurity Act of 2012 (US); Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012 (US).
69 ibid.
70 ibid.
71 Compare House of Commons, ‘Transcript of Oral Evidence taken by the Foreign Affairs Committee, British Foreign Policy and the “Arab Spring”: The Transition to Democracy’, 18 April 2012, HC 1672-V.
The International Strategy for Cyberspace for the US notes that many states put arbitrary restrictions upon the free flow of information or apply restrictions to suppress dissent or opposition activity. Individuals are encouraged to use digital media to express opinions, share information, monitor elections, expose corruption and organise social or political movements, and the US will denounce those who harass, unfairly arrest, threaten or commit violent acts against individuals who use this technology. However, fidelity to the rule of law is simultaneously affirmed. How this strategy proposes to reconcile these sometimes competing objectives is left unsaid.

Furthermore, the proposed Global Online Freedom Act 2012 (US) intends to prevent US businesses from cooperating with governments who use the internet for censorship and repression. ‘Internet-restricting countries’ would be designated for those governments who were directly or indirectly responsible for a systematic pattern involving ‘substantial restrictions on Internet freedom’. By this means the lure of economic assistance displaces the free expression of political opinion in favour of the free availability of electronic information generally.

Here in Australia, around 69 per cent of the population has access to an internet connection at home and around 21 per cent access the internet from their mobile phone. Access to online content is generally unhindered and Australians can openly criticise government policy. Australian law does not currently contemplate the mandatory blocking or filtering of websites, blogs, chat rooms or file-sharing platforms. However, material deemed by the Australian Communications and Media Authority (ACMA) to be ‘prohibited content’ may be subject to ‘take-down’ notices: the relevant internet service provider is notified by the ACMA that it is hosting offending content which must then be removed. Online content which is categorised as ‘Refused Classification’ by the Classification Board is prohibited. Australians are not subject to censorship provided content does not defame or qualify as a criminal offence (such as hate speech or racial vilification). However, verified identification information must be provided to purchase any prepaid mobile telephone service, personal

73 ibid 23–4.
74 ibid 5.
76 Australian Communications and Media Authority, Communications Report 2010–11.
78 Broadcasting Services Act 1992 (Cth).
information is stored while the service remains active and this information can be accessed by law enforcement and emergency agencies upon presentation of a warrant.

As is evident within other states and reflecting global trends, there are emergent threats through regulation to online freedom in Australia. A proposed South Australian election law would have required any individual posting political comments on a blog or online before a local election to use their real name and address. The proposal was withdrawn following a public outcry. Recent amendments to surveillance legislation, accompanied by proposals to implement censorship through directives to internet service providers, have raised concerns about privacy and freedom of expression. In 2010 draft legislation would have required internet service providers to filter illicit content (principally child pornography) and retain data on users’ online activities. This proposed filtering system triggered a number of concerns, including over-blocking, censoring adult materials, ‘scope creep’ and impairing telecommunication access speeds.

As has been observed in Egypt, the UK, the US and elsewhere, political participation can prompt destructive protests which have been organised online through social media tools. Twitter and other social media have cooperated with UK law enforcement in cases of obvious criminality such as rioting, tax avoidance and privacy violations. Australian law enforcement agencies are currently empowered to search and seize computers, and compel internet service providers to intercept and store data from individuals suspected of criminal offences. Internet service providers cannot ordinarily monitor or disclose the content of communications without customer consent. However, intercepting telecommunications is a powerful and cost-effective tool for law enforcement

---

84 ibid. Pt 2–1, s 7 prohibits disclosure of an interception or communication, and Pt 3–1, s 108 prohibits access to stored communications.
authorities and intelligence agencies to counter national security threats and investigate criminal offences. The Australian Federal Police considers that it has a limited ability to lawfully intercept information.

Increased resort to social media tools therefore highlights the familiar problem of regulatory lag. Australian internet service providers may soon be required to monitor, collect and store information pertaining to all users’ communications. The Parliamentary Joint Committee on Intelligence and Security is considering the effectiveness and implications of proposals to ensure that law enforcement, intelligence and security agencies can meet the challenges of new and emerging technology upon their capabilities. Software, ciphers and similar methodologies are being used by organised crime to impede detection by law enforcement authorities. Australia’s intelligence and law enforcement agencies face significant challenges in accessing communications and keeping pace with rapid telecommunications changes. The legal framework also requires updating. For example, the *Telecommunications (Interception and Access) Act 1979* (Cth) assumes that interception can occur at a convenient point within a carrier’s network. However, most contemporary communications networks can be accessed via multiple technologies from many locations and through more than one service provider. The Australian Parliament will shortly be asked how best to balance the protection of individual privacy against the ability of government agencies to access the information necessary to protect the community.

Why then is regulation perceived as a threat to the democratic potential offered by social media, particularly if there are counterbalancing interests at stake? Social media empowers individuals by enabling free expression. Due to its low cost, decentralised nature and great reach, the internet is an important outlet for circulating independent opinions about state authorities and government policies. Many governments have developed an interest in controlling, monitoring

---

and if necessary censoring digital media. As indicated earlier in this chapter, the obvious benefits derived from social media use, including facilitating greater participation by individuals, are not without important qualifications. The desirability of imposing restrictions with a view to protecting privacy, reputations, intellectual property rights, national security or public order can readily be conceded. International human rights law provides only broad normative guidance to regulatory authorities on how respect for the right to freedom of expression is to be ensured and in any event expressly contemplates permissible limitations on its exercise. It ultimately appears that controlling social media can prove technically or politically difficult. Controlling public internet use might require governments to forgo the benefits of connection or expend political capital to block websites. The ‘cute cat theory of digital activism’ posits that governments cannot block political activity without also depriving access to other material, including pictures of cute cats. Governments cannot shut down Facebook, for example, because doing so alienates individuals and might politicise those who lose access.

Social media tools, like other forms of communication, are susceptible to abuse. Its potential to enhance democratic participation should not be overstated. Caution is accordingly appropriate when promoting social media as an instrument for progressive political change. The reality of unequal access and participation between individuals identified above, not to mention ‘digital divides’ between states and the technical challenges confronting government institutions, demands attention. More particularly, governments can subvert the utility of social media platforms by tracking and profiling dissidents, spreading propaganda and establishing false identities in cyberspace (‘sock puppets’) which poison popular trust. Social media can underpin repressive surveillance because data can provide information about a specific dissident and their connections. For example, during 2004 Yahoo provided information to China which helped to identify a dissident blogger, leading to his arrest and imprisonment arising from the content of his online expression.

Efforts to strike an appropriate balance between competing policy priorities in the use of social media, and not simply prioritising political participation, is an emergent regulatory development. Intergovernmental organisations composed of democratic states such as the Council of Europe have recognised that the internet enables people to access information, communicate and participate in

political deliberations. Internet users should be empowered to exercise their fundamental rights and freedoms, make informed decisions and participate in the information society, including developing governance mechanisms and internet-related public policy. However, the Council is also concerned that users tend to use a very limited number of dominant search engines whereby certain types of content or services may be unduly favoured. Those who are responsible for controlling the flow, content and accessibility of information over the internet (‘gatekeepers’) can either facilitate or hinder democratic deliberation and participation. The Council is committed to protecting and promoting access, diversity, impartial treatment, security, transparency and media literacy. Users should also be informed when personal data is used for profiling their behaviour. One non-governmental organisation suggested strengthening the due process protections when blocking and filtering measures were requested by public authorities.

Users of social media have a range of rights and freedoms which are not only limited to political participation. Nor is their interest in expressing opinions or information through a reliable, secure and safe mode of communication limited to social media. The Council of Europe recognises that social media services are human rights enablers and catalysts for democracy. Such services can enhance the participation of individuals in the political, social and cultural life of the state. However, freedom of expression, privacy and human dignity can be threatened by social networking services which shelter discriminatory practices. States should co-operate with the private sector to help users understand the default settings of their profiles, inform users of the consequences of open access to their communications and ensure that users retain the right to limit data access.

94 Council of Europe, Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet (21 September 2011) [3].
97 Council of Europe, Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines (4 April 2012) [6].
98 Council of Europe, Recommendation CM/Rec(2010)13 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling (23 November 2010).
99 Article 19, Response to the Council of Europe Consultation on Search Engines and Social Networking Sites (London, 2011).
100 Council of Europe, Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services (4 April 2012) [2].
Such solutions accompany proposals for global rules which ensure that the internet remains a democratic medium of expression. The protections afforded to journalists, for example, could be extended to online authors. Transparency, openness and accountability are the values to be promoted if political debates are to be enriched. Individuals should be encouraged to participate in the ongoing dialogue on how social media tools are best regulated in the pursuit of democratic ideals. Ensuring that individuals are free to openly discuss the laws governing the conduct of their communities is moreover consistent with ‘deliberative democracy’.

**Conclusions**

Social media can mobilise populations for good or ill. It is conducive to democratisation insofar as this medium has the potential to enhance political participation by individuals. Social media facilitates enjoyment of the right to freedom of expression relatively unhindered by external controls and subject primarily to technological issues such as access and capability. The degree of political participation cannot be left to depend upon such technical aspects given the existence of ‘digital divides’.

Although the utility of social media as a progressive political tool should not be overstated, governments can be made more accountable through this medium. Whereas social media is encouraging greater democratisation within authoritarian states, democratic states including Australia are moving towards tighter regulation. In this context what then is the nature of the conflict between legal restrictions imposed upon freedom of expression and democracy on the one hand, and the appropriate role of social media on the other? Efforts are observable within authoritarian and democratic states to regulate social media for legitimate purposes, such as addressing offensive content or for national security or law enforcement reasons. Governments are also seeking to match increasingly sophisticated communications networks with a more comprehensive surveillance and monitoring apparatus underpinned by law. Thus law inevitably has the potential to necessarily intrude into individual privacy, curtail the enjoyment of other human rights and suppress the democratic potential offered by social media. Stated at its highest, the use by governments of blocking

or filtering technology violates the obligation of states to guarantee freedom of expression. This circumstance reflects the truism that the rule of law and technological determinism are engaged in a constant struggle for supremacy.  

It is not a contest that will soon be resolved, if at all, and the context of social media presents no exception.

---
