Internet Freedom, human rights and power

Madeline Carr*

Internet Freedom is rapidly becoming understood as a normative framework for how the Internet should function and be used globally. Recently declared a human right by the United Nations, it also forms a central pillar of the US 21st Century Statecraft foreign policy doctrine. This article argues that although there is a clear human rights agenda present in this policy, there is also a power element which is much less discussed or acknowledged in the vast literature on Internet Freedom. Through an exploration of both a short history and some important lessons learned about Internet Freedom, this article demonstrates how the US Department of State has adapted to the information age in such a way as to harness individual agency (reconceptualised in policy terms as 'civilian power') for the promotion of state power. Although this is by no means as stable or reliable as some more conventional mechanisms, it is an expression of power that meets with few challenges to its legitimacy.

Keywords: Internet Freedom: 21st Century Statecraft; US power; Internet censorship; social construction of technology; miliblogs; civilian power

Introduction

Internet Freedom is rapidly becoming understood as a normative framework for how the Internet should function and be used globally. In June 2012, it was declared a human right by the United Nations Human Rights Council. The *Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet* (UNHRC 2012) calls on all states to promote and facilitate access to the Internet and to ensure that the same rights of freedom of expression that are available offline are protected and upheld online. There has been a strong global civil society movement to promote Internet Freedom—a norm that has been deeply embedded in the 'culture' of Internet technology from the 1980s. Organisations like the Open Net Initiative and the Electronic Frontier

* Madeline Carr is Lecturer in International Politics and the Cyber Dimension in the Department of International Politics, Aberystwyth University. <madeline.carr@aber.ac.uk>.

Foundation work to identify and report on Internet censorship, filtering and surveillance. In addition to being regarded as an important principle and now a human right, Internet Freedom has been a central pillar of the US 21st Century Statecraft foreign policy doctrine, developed by former US Secretary of State, Hillary Clinton. Through an analysis of Internet Freedom in US foreign policy, this article argues that Internet Freedom can be understood not only as the promotion of human rights or of a normative 'public good' but also as an expression of state power.

There is some political tension around Internet Freedom because it can conflict with the requirements of cyber-security (as has become clear in the wake of the Prism controversy in the US). The right to online privacy, and to view, write or interact free of surveillance is a deeply held and fiercely protected norm in many states. However, anonymity and the consequent difficulty in attribution of illegal online activity are deeply problematic from a cyber-security perspective—even in these same states. The same qualities of the Internet that afford anonymity to anti-social actors engaging in theft, espionage or disruptive behaviour also provide cover for political activists in non-democratic states who wish to voice their ideas and collaborate with other like-minded citizens. The difficulty of online attribution is both a *problem* for state security and a *safeguard* for global civil society. Not surprisingly, balancing these imperatives of privacy and security is difficult and approaches to finding this balance vary widely. This is complicated further by the fact that although challenges to cyber-security are valid, some states that object to Internet Freedom arguably use cyber-security as a mask for deeper concerns about regime stability in the face of anonymity and freedom of political speech online (Deibert *et al.* 2011).

The growing literature on Internet Freedom has focused almost exclusively on those states that overtly censor information, monitor online activities of individuals and/or limit access to certain sites in contravention of the principle of Internet Freedom. Less examined have been the ways in which policymakers in liberal democracies approach Internet Freedom where it resonates with ideas about individual agency, privacy, transparency, and freedom of information - all of which are intimately linked to government legitimacy. In states where these liberal ideas are deeply embedded, accommodating the changes that Internet technology has introduced in terms of state control over information has clearly been less of an adjustment than in states where civil

society has not yet established the same expectations of transparency and freedom of access to information. In effect, in liberal democracies the challenges of adapting to the information age were eased by pre-existing expectations of offline rights. However, even for these states the adaptation has not been seamless and governments have had to confront and adjust to change through developing new policy, law and practices—many of which are now being guided by the principles of Internet Freedom.

Acknowledging and discussing the power component of Internet Freedom is important for a number of reasons. First, a particular set of norms is being built into the institutions, processes and principles that, to a significant extent, determine the way the Internet functions, is governed and develops. In this context, the promotion of Internet Freedom has not only become a dimension of US foreign policy, but also an expression of US structural and institutional power. In much the same way as the Bretton Woods agreement set in place the structure of the global economic system after the Second World War, so too are decisions and arrangements about the Internet laying down the pathways for how actors may legitimately engage with Internet technology in the future. This is neither good nor bad, but it is worthy of close analysis. All states may be expected to promote an online ecosystem that reflects their interests, principles and values and Internet Freedom is emerging as an important element in this practice for the US.

Another important reason to acknowledge the power component of Internet Freedom is because it can enhance our understanding of why some states resist the adoption of the human rights element of Internet Freedom. Just as the Iraq war has undermined the legitimacy of the 'Responsibility to Protect' initiative by blending human rights and national interest, the power component of Internet Freedom may be overshadowing the human rights agenda for some states. Finally, and related to the previous point, by understanding the way the US has conceived of this form of power, reluctant states may be influenced to reconsider the benefits of adopting Internet Freedom in some form. Although motivated by these observations, this article does not build an argument around these factors. Its more modest aim is to lay the conceptual groundwork for further investigation into them by establishing that there *is* a component of power in US conceptions of Internet Freedom.

This article proceeds in three parts. The first section briefly details the development of Internet Freedom as a human right in the US by tracing its political history as a civil right. This section demonstrates a clear link between Internet Freedom, human rights and liberal ideas about individual rights in order to clearly establish the authenticity of the human rights agenda in Internet Freedom. In the following two sections, the article explores two key sites that both demonstrate and further shape US approaches to Internet Freedom and power. The first of these two examples provides an analysis of the US Department of Defense's (DoD) response to military blogging (miliblogs) in the mid-2000s. This case predates notions of an explicit link between power and Internet Freedom as a foreign policy, and can therefore help to explain its evolution. As a policy approach, Internet Freedom has important antecedents that impacted significantly on US approaches to the control of information during war and political conflict. An analysis of policy shifts around military blogging is an effective way to demonstrate this empirically.

In the second of these examples (and the third main section of the article), Internet Freedom as an element of power within the doctrine of 21st Century Statecraft is explored through the concept of 'civilian power'—arguably an outcome of the learning experience of dealing with military blogging in the US. Through an analysis of US foreign policy during the 'Arab Spring'—a major 'laboratory' for examining the doctrine of 21st Century Statecraft – and theoretical concepts drawn from the philosophy of technology, this section provides insight into how US policymakers approach Internet technology in the context of ideas about the expression of US power.

The article concludes by reaffirming that it would be inaccurate to suggest that Internet Freedom is without ideological support in the US, but that it has also been incorporated into a new approach to power in the information age. This element of power may go some way to explaining why some states may regard the foreign policy of Internet Freedom as the establishment of a new US led hegemonic framework for how the Internet should operate, be governed and develop in the future.

Internet Freedom as a human right

As explained earlier the argument in this article is not that Internet Freedom is simply power disguised as ideology; rather, it represents a confluence of both. Extensive

analysis of two decades of transcripts of Congressional hearings into cyber security reveals that even in the face of considerable concern about security vulnerabilities, US politicians tended to privilege privacy and freedom of information (Carr 2011). However, when they do so, they frequently make reference to US power as *emerging* from these values and principles. That is, they regard US power as contingent upon the political will to adhere to the kind of 'moral framework' which they feel makes that state exceptional. The following section very briefly traces the emergence of Internet Freedom as a human right in the US over the past two decades while acknowledging that the antecedents of norms about freedom of information, privacy and individual rights go back well beyond Internet technology.

In the early years of the Internet, the Bill Clinton–Al Gore administration focused predominantly on the domestic promise of a fully developed and implemented information infrastructure. Protecting civil rights was already regarded as critical even as awareness of security problems grew (Gore 1993, 1994). A 1995 General Accounting Office report identified several services which it argued would be essential for network security in the future. They included: 'identification and authentication—the ability to verify a user's identity and a message's authenticity', and 'nonrepudiation—the ability to prevent senders from denying they have sent messages and receivers from denying they have received messages' (Willemssen 1995: 20). These policies, if implemented, might have profoundly reshaped cyber-security technology, but in the US, they could not be reconciled with the values and principles associated with civil liberties and were never passed.

Internet technology increasingly came to be seen as synergistic with a foreign policy based on liberalisation of trade, democratic enlargement and the promotion of human rights. By 1999, the concept of promoting human rights abroad and the relevance of the Internet in that pursuit united in the *National Security Strategy* which listed information and communications technology as key to mitigating human rights abuses and promoting the free flow of information (Clinton 1999: 26). In 2000, the US government produced the first national plan for the protection of the information infrastructure, *Defending America's Cyberspace.* In it, the emphasis on the ideas behind Internet Freedom as a civil liberty continued to evolve and act as a counter-weight to security concerns (Clinton 2000: v). This duality of security and privacy is

acknowledged throughout the document, but ultimately it argues that 'while safeguarding our critical infrastructures is vital, protecting our civil liberties is paramount' (Clinton 2000: xxxvi).

During George W. Bush's presidency, the concept that access to the Internet was a human right which should be promoted globally continued to develop. A number of Bills were introduced (although not passed) designed to combat state sponsored censorship and monitoring of Internet use. The *Global Internet Freedom Bill* expressed the view that the United States should 'denounce governments that restrict, censor, ban, and block access to information on the Internet' and 'deploy technologies aimed at defeating state-directed Internet censorship and the persecution of those who use the Internet'. [1] US government efforts to defeat the blocking of Internet access included funding to provide counter-censorship software to Internet users in places like China (Lum 2006). This, it was argued, would enable citizens of these states to 'exercise their most basic rights' by using the Internet to communicate with each other and with the outside world (Kellerhals 2010).

In January 2010 during a speech at the Newseum in Washington, Hillary Clinton identified Internet Freedom as a central pillar of her 21st Century Statecraft doctrine. Referring to information networks as 'a new nervous system for our planet', she outlined the ways in which access could make societies stronger, hold governments accountable and help to promote the struggle for 'freedom and progress' (Clinton 2010). The 21st Century Statecraft doctrine links the Internet to human rights in two ways. First, it perpetuates the approach developed over the previous decade that access to the Internet should be regarded as a civil and human right. In this context, Clinton repeatedly linked the Internet to the *Universal Declaration of Human Rights*. Clinton then expanded this to define the Internet as a new 'site' of human rights abuses which is derived from what she dubbed the 'freedom to connect'—like the freedom of assembly, only in cyber-space: 'I talked about how we must find ways to make human rights a reality. Today, we find an urgent need to protect these freedoms on the digital frontiers of the 21st century' (Clinton 2010).

Clinton exhibited a sophisticated approach to the inter-relationship between competing expectations of privacy and security in Internet technology. Rather than

ignore or play down these contradictions, she acknowledged and confronted them. In her second major speech about Internet Freedom, Clinton argued that

> liberty and security, transparency and confidentiality, freedom of expression and tolerance—these all make up the foundation of a free, open, and secure society as well as a free, open, and secure Internet where universal human rights are respected, and which provides a space for greater progress and prosperity over the long run (Clinton 2011c).

Her approach to finding a balance between these sometimes competing demands has been to limit the 'universality' of this particular human right. After outlining the many advantages which Internet technology offers to the projection of US foreign policy in the Newseum speech, Clinton also remarked that 'these technologies are not an unmitigated blessing' because the same technologies which promote human rights also allow groups like al-Qaeda to operate globally (Clinton 2010).

In fact then, Internet Freedom as US foreign policy is a view which maintains that this human right is not as universal as some. While we might regard everyone, even al-Qaeda operatives, to be entitled to 'basic' human rights like food, shelter and medical treatment regardless of the crimes they may commit, their right to Internet Freedom is contingent—in fact, it is deeply political. E. H. Carr (1964: 11) argued that utopia and realism were the two essential elements of political discourse—that one without the other was inadequate. This is perhaps what we see in Clinton's Internet Freedom speech—an aspiration to promote liberal norms and values that are understood to be the foundations of a freer and more equitable world, coupled with the acknowledgement of the reality that some limits on this right can best promote and protect US interests. In establishing a clear link between Internet Freedom as a 'non-basic' human right and as related to US power, she also argues that '[t]hose who disrupt the free flow of information in our society or any other pose a threat to our economy, our government, and our civil society' (Clinton 2010). Ultimately, Clinton observes that the US will have to struggle to balance ideational and material power concerns in this context.

The power component of Internet Freedom is further examined later in this article. First though, it is useful to look at an empirical example that pre-dated Clinton's Internet Freedom policy. In the mid-2000s, military blogging brought the notion of access to the Internet as a civil right into conflict with imperatives of state security. An

analysis of how US policymakers responded to this allows us to consider what impact this learning experience had on future approaches to Internet Freedom, human rights and power.

Internet Freedom in transition: Miliblogs

Internet Freedom is particularly interesting to analyse during times of war and political conflict because this can be a time when governments, even in liberal democracies, are tempted to exercise greater control as part of a broader strategy of managing a crisis. It is a time when cracks can appear in an otherwise cohesive policy approach to these issues. In states with a less than free media, governments have more flexibility to control the flow of information and public communication. Liberal democracies that have a (relatively) healthy, functioning media face a different set of challenges. This has been explored comprehensively through the literature following the Vietnam War and further developed in a second wave of analysis looking at the revised US strategies of embedding journalists in the first and second Iraq wars (Aday et al, 2005; Hieber 2003; Pfau 2004). For many, these new approaches were regarded as an effort to maximise control over information about the conflict while simultaneously giving the impression of transparency. Much of the literature around these practices and approaches is based on the understanding that freedom of information and governmental transparency are linked to legitimacy in liberal democracies (Bell 2008; Dodson 2010; Paul and Kim 2004).

In the 2000s, the US Department of Defense (DoD) faced a new challenge when soldiers serving on the frontlines in Iraq and Afghanistan began communicating to family, friends and strangers through blogs. Coined ‘miliblogs’, these are typically unedited, uncensored and deeply personal blogs written by soldiers to express views that can differ quite significantly from broader institutional perspectives of either the Department of State, the DoD or the conventional media.

In 2003, US infantryman Colby Buzzell began anonymously blogging about his experiences in Iraq. Buzzell’s blog was funny and irreverent, but it also dealt candidly with both his fear and boredom, and his general bewilderment at why he and his colleagues were fighting in a desert across the globe from his home state. [2] His frank and articulate account was quickly picked up by the online community generating

hundreds of response emails a day (Cammaerts and Carpentier 2009). Buzzell's blog offered a fresh account of a war largely reported by embedded journalists existing on a drip feed of information and images controlled by the military.

Military policy on social networking media at the time that Buzzell was blogging was unequivocal. Miliblogs were regarded as a security threat and an unauthorised release of information and images (Sipress and Diaz 2007). In 2005, a series of DoD memos were issued to coincide with military orders to restrict access to sites including Facebook, YouTube and MySpace. General Richard Cody wrote that:

> The enemy is actively searching the unclassified networks for information, especially sensitive photos, in order to obtain targeting data and weapons system vulnerabilities for use against the coalition. A more aggressive attitude toward protecting friendly information is vital to mission success (Cody 2005).

Some soldiers continued to blog, but a number received an 'Article 15' non-judicial punishment and/or fines or demotions for posting material deemed sensitive. (Ambrosio 2005).

In 2007, following a significant and negative civil society response to the social media ban, the US military underwent a policy 'about face' with the use of miliblogs not only allowed but actively encouraged, and indeed incorporated into staff training curriculums. (Whitelaw 2009). General David Petraeus wrote to thank 'the bloggers who have worked to provide accurate descriptions of the situation on the ground here in Iraq and elsewhere' (cited in Shachtman 2007). In response to questions about the reversal in policy towards miliblogs, Army Public Affairs Spc. Lindy Kyzer explained that 'We're actually entering an era of transparency, where we need to have our soldiers talk … They are our best spokespersons' (Griggs 2009).

While it is possible that improving transparency was a motivating factor, even in liberal democracies the military is not a context in which transparency is expected to trump either national security or the security of soldiers' lives. Lt. Gen. William Caldwell perhaps made a more salient point when he said that '[a]cross America, there is a widely held perception that media coverage of the War in Iraq is overwhelmingly negative' and to counter this:

> we must encourage our Soldiers to interact with the media, to get onto blogs and to send their YouTube videos to their friends and family. When our

> Soldiers tell/share their stories, it has an overwhelmingly positive effect (Caldwell 2008).

Petraeus endorsed this view. Milibloggers, he argued, had become increasingly important in the context of a shift from conventional news outlets to online news sources. 'Your efforts strengthen the bonds of the military community' (cited in Shachtman 2007).

In fact, this case reveals a 'learning experience' in the US about options for liberal democracies to better synergise security and individual human rights—not through the *control* of information which quickly elicited significant approbation from the US public, but by recognising that individual agency that is broadly in harmony with US foreign policy interests can be a powerful propellant. Miliblogs certainly contain plenty of negative messages—about fear, loneliness, frustration and the tedium of war— but it had become clear that the connections forged between blogging soldiers and the US population had a *positive* effect on domestic support for the war. (Matheson and Allan 2007). Although it continues to have a somewhat troubled and conflicted relationship with social networking media (Corrin 2012; Dao 2009), the DoD found that the negative views expressed by some soldiers were offset by the fact that miliblogs significantly strengthened public identification with soldiers, and thereby reinforced domestic support for the war. This was an unintended but highly valued consequence.

The concepts and ideas behind Internet Freedom as a foreign policy — that harnessing individual agency in order to promote US interests could be an effective alternative to the direct control exercised by less liberal states—resonates with this learning experience of the DoD during the early years of social networking media. The DoD initially regarded *agency* as the same as *power* in this setting. The initial restrictive policy response indicated an assumption that individual soldiers with the agency to disseminate information about the war zone detracted power from the DoD. In fact, they found that harnessing individual agency in the form of miliblogs not only enhanced DoD legitimacy (as it was seen to be progressive, transparent and open), but could serve to promote the agenda of the DoD through generating domestic support for the war effort. This approach to controlling information—or rather, in recognising the multiple benefits of *not* controlling it—for the promotion of US power was later united with the previously discussed and deeply held notions of Internet Freedom as a civil/human

right. Together, they were united in the concept of 'civilian power' in the 21st Century Statecraft doctrine.

Internet Freedom as US power

Secretary of State Clinton's doctrine of 21st Century Statecraft articulates a view of US power which is closely integrated with information and communications technology. The emphasis of 21st Century Statecraft is on 'people to people' diplomacy in recognition of the view that diplomatic outcomes are not defined solely by what elites prefer, but also by what the general population strives for. A key element of this approach is the understanding that civil society can become a catalyst for change in any state and this is linked to the projection of US power. As articulated in the *Quadrennial Diplomacy and Development Review* 'fact sheet': 'to advance American interests and values and to lead other nations in solving shared problems', the US must rely not only on diplomats but also on 'civilian experts as the first face of American power' (US Department of State and USAID, no date). This is referred to by the Department of State as 'civilian power', and it forms the bedrock of 21st Century Statecraft.

'Civilian power' can be conceptually linked to Joseph Nye's work on 'soft power' and 'smart power' (Nye 2004; Nye and Armitage 2007). It would appear (to some degree at least) to be an approach that decouples agency from power, or at least regards agential power as 'non-zero sum'. That is, agency previously concentrated in state instruments *may* expand to include civil society, but contrary to many current conceptions, power does not necessarily follow in a direct and related equation. The diffusion of agency does not necessarily and unequivocally lead to a diffusion of power—thereby weakening the traditional centre of power in the state. Soldiers may be awarded the agency to communicate their own individual view of the war to a global audience, but power was not necessarily transferred away from the state in this transaction.

Less than a year after Clinton outlined her vision for 21st Century Statecraft and Internet Freedom, events in the Middle East provided an ideal opportunity to observe these ideas in the context of political conflict through the 'Arab Spring' uprisings. Unlike the case of miliblogs, controlling and countering negative messages was not the primary challenge for the US here. The flow of information across social networking

sites was overwhelmingly supportive of the protestors—and largely in line with US foreign policy objectives. The literature around the use of social networking technology during the Arab Spring uprisings is extensive and predominantly revolves around the debate about whether social networking media had a significant role to play in the regime changes that followed or not (Gladwell 2010; Goodin 2011; Morozov 2011; Mourtada and Salem 2011; Shane 2011; Ward 2011;). Rather than re-engage with this debate, the following section provides analysis of the ways in which Secretary Clinton and her senior policy advisors approached and interpreted this debate.

The 'philosophy of technology' provides a set of concepts useful for analysing political approaches to technology. Two are particularly evident in the broader debates around Internet Freedom during the Arab Spring; a *determinist* approach to technology and a *social constructivist* approach to technology. These approaches have different policy implications (the first, laissez-faire and the second, interventionist), and they suggest different approaches to the power of technology (the first, autonomous and the second, human directed). A determinist approach to technology removes human agency (and therefore responsibility) and locates it instead in the technology itself, while a social constructivist approach regards technology as fundamentally shaped by human defined expectations, perceptions and, significantly for this article, power (Bimber 1990; Kraft and Vig 1988; MacKenzie and Wacjman 1999; Pinch and Bijker 1989; Winner 1985). The following pages explain how and why US policymakers have laid claim to a determinist approach while actually pursuing the policies dictated by a social constructivist approach. This is not simply an academic exercise in determining how the philosophy of technology fits into this empirical material. It is essential in order to deconstruct how these policymakers regard US power and Internet Freedom in the context of the Arab Spring events.

Internet Freedom: A Digital Che Guevara?

The public face of the Department of State's new media policy had for some time been Jared Cohen and Alec Ross—two young diplomats who had been influential in formulating policy around Internet technology. Ross, Senior Advisor for Innovation expressed some definite ideas about the relationship between the Internet (social networking media in particular), power and agency in international relations. In keeping

with a determinist approach, Ross regarded the technology itself as having agency, referring to the Internet as 'the Che Guevara of the 21st Century'. Furthering the revolutionary metaphor, Ross argued that 'connection technology takes power away from the nation-state and … gives it to individuals' (Ross 2011).

In this determinist view, the Internet is an autonomous actor that reassigns agency and power in international relations. During this period, the Department of State was promoting the message that these events were a natural and probably inevitable outcome of new democratising technology. The US (it was argued), was simply an observer of these events with real agency resting in Arabic 'civilian power' through Internet Freedom (Clinton 2011a, 2011b; Crowley 2011). Prominent theorist Langdon Winner has argued that by imbuing technology with agency and purpose, we may deny having it ourselves, and therefore be released from the burden of accountability (Winner 1985).

Framing the role of Internet and mobile technology in the Arab Spring uprisings in a determinist approach to technology served to insulate (to some extent) the Department of State from accusations of actively promoting regime change. However, there were explicit contradictions to this view evident in the fact that the Department of State funded the development of technological tools to help individuals avoid government restrictions and surveillance in a number of these states. This suggests a belief that technology *can* be shaped and directed to achieve political goals—it is not autonomous as in Ross's 'Che Guevera' analogy. Rather, it is a tool for social and political reform. This is an approach to technology that puts agency back in the hands of those with power to shape it—a social constructivist approach to technology.

Internet Freedom and Political Reform

An important element of the promotion of Internet Freedom has been the control of technological tools supplied to states where online human rights have been perceived as lacking. This refers first to the funding and provision of technology that helps activists and protesters to evade detection and circumvent government restrictions on Internet access. It also refers to US restrictions on sales of surveillance and tracking tools to these governments (Horwitz, Asokan and Tate 2011). In Clinton's first speech on Internet Freedom in 2010, she outlined the supply side of this policy:

> We are also supporting the development of new tools that enable citizens to exercise their rights of free expression by circumventing politically motivated censorship … [w]e want to put these tools in the hands of people who will use them to advance democracy and human rights (Clinton 2010).

There is an expectation here that 'civilian power', if provided the right tools, will bring about political change.

Again, the policy framework for this funding program allows us to observe the relationship between Internet Freedom as a human right and as an expression of state power. It is a relationship that produces both tension and accord. Ross clearly contradicts Clinton's view by arguing that the many tools funded and developed by the Department of State to circumvent political control over the Internet are *not* aimed at activists—rather they are developed with 'everyday citizens' in mind in the drive to ensure their human rights are upheld (Ross 2012). This may be a subtle distinction but it is an important one. In Ross's view, technological tools are developed and delivered to everyone as a means of facilitating their human right to Internet access. Whether that leads to political change is immaterial because the provision is a human rights issue. In Clinton's view, these tools are targeted at those political actors who might be expected to use them to bring about political change and this demonstrates belief in a strategic element of Internet technology. In a 2012 address, State senior official Michael Posner was clear that Internet Freedom was *not* to be linked to aspirations of regime change in US foreign policy. 'We don't promote Internet freedom or connective technologies as a means of promoting "regime change." We promote the freedoms of expression, association and assembly online and offline because these universal freedoms are the birthright of every individual' (Posner 2012). One may take Ross and Posner at their word (and why not—Internet Freedom as discussed earlier has a legacy of civil/human rights in the US), but by funding technology that allows citizens to avoid the scrutiny of their governments and by prohibiting the sale to certain states of surveillance technologies used freely in the West, Internet Freedom comes to be perceived by others as an expression of US power.

A more recent development helps to illustrate this point about how far Internet Freedom is extended in its conception as a US foreign policy implement. Iranian media

faced sanctions through a Bill passed in the US Senate in November 2012. The Islamic Republic of Iran Broadcasting (IRIB) was accused in the text of the Bill as having infringed upon the rights of individuals' human rights by 'broadcasting forced confessions and show trials' (S.3254 2012: 801-2). IRIB had been dropped six weeks earlier from the Eutelsat owned satellite service after pressure from the European Union and France's broadcasting authority (BBC News 2012; Eutelsat Communications 2012). The irony of Iran's broadcasting services being restricted under the auspices of Internet Freedom links back to lessons from miliblogs. If soldiers writing from the frontlines of their miserable conditions could generate public support for the war effort, what effect might greater exposure to an Iranian perspective have on global civil society? Ross had spoken about the Iranian media ecosystem earlier in the context of the Department of State's effective use of Twitter. Tweeting in Farsi, he noted, had allowed the US to reach the Iranian people directly without the Iranian government 'mucking around our messages' (Ross 2011). It seems the reverse is not to be, and in the interests of Internet Freedom, an Iranian voice will not be heard in the West.

Finding contradictions in policies like Internet Freedom is not particularly difficult and nor (when isolated) is it particularly interesting. However, examining *why* there are contradictions in this case can highlight the tension between Internet Freedom as a human right and Internet Freedom as an expression of state power. Whether the funding, distribution and restriction of technological tools is directed toward activists as Clinton argues, or 'everyday citizens' as Ross and Posner suggest, it is evident that despite a diffusion of agency to civil society, the power of the Department of State to direct Internet technology to promote a foreign policy agenda remains intact. Whether IRIB has been restricted for Western audiences as a means of objecting to human rights abuses or because it undermines the interests of the US (and the European Union), it allows us to observe the boundaries of Internet Freedom as a universal human right. Contrary to Ross's determinist arguments, technology can be purpose built and delivered in such a way as to bring about change. A budget of US$100 million for the development of supplied Internet Freedom technology between 2008 and 2012 makes it difficult to continue to argue that this is simply 'bottom up' change—and not to some extent at least, also top down (Hanson 2012).

Conclusion

The link between conceptions of civil and human rights and the foundations of the US policy of Internet Freedom is clear and uncontroversial. That there is also a power component to the policy is less discussed and more contentious. The evolving view that Internet Freedom was a civil and then a human right, forced the US DoD to confront the way it dealt with soldiers' communiques in the context of the information age. The shift from one-to-one personal communication (letters, phone calls and even email) to one-to-many (blogs), meant that questions of agency, control and security needed to be re-evaluated. The lesson from military blogging was not simply that social networking is an unstoppable force for individual empowerment, a force to which powerful actors would have to bend. Nor did it signal a fundamental shift to a more transparent era for the US military. Rather, the substantive lesson from military blogging was that individual agency could work to institutional advantage. If some negative effects were tolerated, the positive impact of allowing open communication between soldiers and the US domestic population was considerable. In fact, it was more powerful than conventional media in generating support for the war effort.

This lesson was significant enough to be later extrapolated beyond the setting of the DoD to being influential in the formation of Internet Freedom as part of a key foreign policy under Clinton's term as Secretary of State. The US Department of State and the DoD have adapted to the information age in such a way as to globally harness individual agency (reconceptualised in policy terms as 'civilian power') for the promotion of US power. Although this is by no means as stable or reliable as some more conventional mechanisms, it is an expression of power that meets with few challenges to its legitimacy.

The combination of human rights and the projection of US power produces the same problems of legitimacy for Internet Freedom that the Iraq war has introduced for the 'Responsibility to Protect' concept. Walking a line between the promotion of human rights and the correlating promotion of US interests and power is a difficult balance and one which unfortunately can serve to undermine an authentic human rights agenda. Certainly, Clinton has been criticised for the contradictions inherent in Internet Freedom which ascribes freedom of access and freedom of information—but not to those who would do harm to US interests. In fact, it could be argued that her policy represents a

sophisticated and realistic attempt at squaring the circle of competing demands of transparency and security faced by liberal democracies in the information age.

The problem is that while she may find consensus on the need to balance civil liberties and security from all governments, the devil is undoubtedly in the nuance. Different perceptions of who is entitled to Internet Freedom and who is not, between what online activity threatens state interests and what does not, even between how to define state interests, means that ultimately Internet Freedom remains subjective and contextual. Power in the information age will to some extent be defined by which version of Internet Freedom prevails over the others.

Notes

1. This Bill was introduced to the 107th Congress as HR 5524. It was reintroduced as HR 48 in 2003. In addition there was a Senate version in the 107th Congress numbered S 3093, co-sponsored by Senator Ron Wyden and Senator Jon Kyl.

2. Buzzell's original blog is no longer available online but a compilation of his blog postings and other writing has been published in a manuscript. See Buzzell (2006). For his current blog, see <cbftw.blogspot.co.uk/>.

References

Aday, Sean, Steven Livingston and Maeve Herbert. 2005. "Embedding the Truth: A Cross-Cultural Analysis of Objectivity and Television Coverage of the Iraq War." *International Journal of Press/Politics* 10(1): 3-21.

Ambrosio, Johanna. 2005. "Milblogs: A Very Thin Line Indeed." *InformationWeek*, 27 September, <www.informationweek.com/news/171200867>.

BBC News. 2012. "EU Imposes New Sanctions on Iran." 15 October, <www.bbc.co.uk/news/world-middle-east-19947507>.

Bell, Martin. 2008. The Death of News." *Media, War & Conflict* 1(2): 221-31.

Bimber, Bruce. 1990. "Karl Marx and the Three Faces of Technological Determinism." *Social Studies of Science* 20(2): 333-51.

Buzzell, Colby. 2006. *My War: Killing Time in Iraq.* New York: Random House.Caldwell, Bill. 2008. "Changing the Organizational Culture (Updated)."

Small Wars Journal, 3 February, <smallwarsjournal.com/blog/changing-the-organizational-culture-updated>.

Cammaerts, Bart and Nico Carpentier. 2009. "Blogging the 2003 Iraq War: Challenging the Ideological Model of War and Mainstream Journalism?" *Observatorio (OBS*)* 3(2): 1-23.

Carr, Edward Hallett. 1964. *The Twenty Years' Crisis, 1919-1939*. New York: Perennial.

Carr, Madeline. 2011. "The Irony of the Information Age: US Power and the Internet in International Relations." PhD diss., Australian National University.

Clinton, Hillary. 2010. "Remarks on Internet Freedom." The Newseum, Washington, DC, 21 January, <www.state.gov/secretary/rm/2010/01/135519.htm>.

Clinton, Hillary. 2011a. "Interview with Candy Crowley of CNN's State of the Union." Washington, DC, 30 January, <www.state.gov/secretary/rm/2011/01/155588.htm>.

Clinton, Hillary. 2011b. "Interview with Christiane Amanpour of ABC's This Week." Washington, DC, 30 January, <www.state.gov/secretary/rm/2011/01/155586.htm>.

Clinton, Hillary. 2011c. "Internet Rights and Wrongs: Choices and Challenges in a Networked World." George Washington University, Washington, DC, 15 February, <www.state.gov/secretary/rm/2011/02/156619.htm>.

Clinton, William J. 1999. *United States National Security Strategy*. Washington, DC: The White House.

Clinton, William J. 2000. *Defending America's Cyberspace: National Plan for Information Systems Protection*. Washington, DC: The White House.

Cody, Richard A. 2005. "Sensitive Photos." US Army Memo DTG: 141637Z 5 February, <www.fas.org/sgp/news/2005/08/usa0805.html>.

Corrin, Amber. 2012. "DOD's New Policy 'Likes' Social Media, but with Caveats." *Federal Computer Weekly (FCW)*, 14 August, <fcw.com/articles/2012/08/15/feat-inside-dod-social-media-policy.aspx>.

Crowley, Philip J. 2011. "Current Global Events and Trends." Washington, DC, 20 January, <fpc.state.gov/155031.htm>.

Dao, James. 2009. “Leashing the Blogs of War.” *New York Times,* 8 September, <atwar.blogs.nytimes.com/2009/09/08/leashing-the-blogs-of-war/?ref=us>.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. 2012. *Access Contested: Security, Identity, and Resistance in Asian Cyberspace.* Cambridge, MA: MIT Press.

Dodson, Giles. 2010. “Professional Discourse and the Legitimation of the 2003 Iraq Invasion.” *Australian Journalism and War* 11(1): 99-114.

Eutelsat Communications 2012. “Eutelsat Statement on Islamic Republic of Iran Broadcasting (IRIB).” Paris, 15 October,. <www.eutelsat.com/news/compress/en/2012/pdf/Eutelsat%20Statement%20on%20IRIB.pdf>.

Gladwell, Malcolm. 2010. “Small Change: Why the Revolution Will Not Be Tweeted.” *The New Yorker,* 4 October, <www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell>.

Goodin, Dan. 2011. “Internet Use Disrupted in Bahrain as Protests Turn Bloody.” *The Register,* 18 February, <www.theregister.co.uk/2011/02/18/bahrain_internet_disruption/>.

Gore, Albert Jr. 1993. “Remarks at the National Press Club.” Washington, DC, 21 December.

Gore, Albert Jr. 1994.“Remarks at Royce Hall, UCLA.” Los Angelos, 11 January.

Griggs, Brandon. 2009. “Soldier Finds His Voice Blogging From Iraq.” *CNN,* 23 January, <edition.cnn.com/2008/TECH/11/13/soldier.blogger/index.html>.

Hanson, Fergus. 2012. “Internet Freedom: The Role of the US State Department.” *Brookings,* 25 October, Washington, DC, <www.brookings.edu/research/reports/2012/10/25-ediplomacy-hanson-internet-freedom>.

Hieber, Ray Eldon. 2003. “Public Relations and Propaganda in Framing the Iraq War: A Preliminary Review.” *Public Relations Review* 29(3): 243–55.

Horwitz, Sari, Shyamantha Asokan and Julie Tate. 2011. “Trade in Surveillance Technology Raises Worries.” *Washington Post,* 1 December, <articles.washingtonpost.com/2011-12-01/world/35286192_1_surveillance-technology-first-trade-show-products>.

Kellerhals, Merle David Jr. 2010. "US Treasury Opens Internet Exports to Iran, Sudan, Cuba." *America.gov,* 12 March, <www.america.gov/st/democracyhr-english/2010/March/20100312160116dmslahrellek0.7673914.html>.

Kraft, Michael E. and Norman J. Vig, eds. 1988. *Technology and Politics*. Durham and London: Duke University Press.

Lum, Thomas. 2006. "Internet Development and Information Control in the People's Republic of China." Washington, DC: Congressional Research Service, 10 February, <www.fas.org/sgp/crs/row/RL33167.pdf>.

MacKenzie, Donald and Judy Wajcman, eds. 1999. *The Social Shaping of Technology.* Philadelphia: Open University Press.

Matheson, Donald and Stuart Allan. 2007. "Truth in a War Zone: The Role of Warblogs in Iraq." In *Communicating War: Memory, Military and Media,* edited by Sarah Maltby and Richard Keeble, 75-89. Bury St Edmunds: Arima.

Morozov, Evgeny. 2011. *Net Delusion: The Dark Side of Internet Freedom.* New York: PublicAffairs.

Mourtada, Racha and Fadi Salem. 2011. "Civil Movements: The Impact of Facebook and Twitter." *Arab Social Media Report* 1(2). Dubai: Dubai School of Government, Governance and Innovation Program. <www.dsg.ae/en/ASMR2/Images/report.pdf>.

Nye, Joseph S. 2004. *Soft Power: The Means to Success in World Politics*. New York: PublicAffairs.

Nye, Joseph S. and Richard L. Armitage. 2007. *CSIS Commission on Smart Power: A Smarter, More Secure America.* Washington, DC: Center for Strategic and International Studies.

Paul, Christopher and James J. Kim. 2004. *Reporters on the Battlefield: The Embedded Press System in Historical Context.* Santa Monica: Rand Corporation.

Pfau, Michael. 2004. "Embedding Journalists in Military Combat Units: Impact on Newspaper Story Frames and Tone." *Journalism and Mass Communication Quarterly* 8(1): 74-88.

Pinch, Trevor E. and Wiebe E. Bijker, eds. 1989. *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA: MIT Press.

Posner, Michael H. 2012. “Internet Freedom and the Digital Earthquake of 2011.” Remarks to the State of the Net Conference, Washington, DC, 17 January, <www.state.gov/j/drl/rls/rm/2012/180958.htm>.

Ross, Alec. 2011. “Alec Ross on the Impact of the Social Media.” Interview produced by the Embassy of United States Public Diplomacy Section, Brussels, 6 March, <www.youtube.com/watch?v=BcywfhtvYl4>.

Ross, Alec. 2012. “Internet Freedom: An Interview with Alec Ross.” Brookings Institution, 16 April, <www.youtube.com/watch?v=xVqf2DeS9ro&feature=relmfu>.

S.3254 2012. National Defense Authorization Act for Fiscal Year 2013, US Senate, December,. <www.gpo.gov/fdsys/pkg/BILLS-112s3254es/pdf/BILLS-112s3254es.pdf>.

Schoomaker, Peter J. 2005. “Chief of Staff of the Army OPSEC Guidance.” US Army Memo P 231903Z 5 August, <www.fas.org/sgp/news/2005/08/usa0805.html>.

Shachtman, Noah. 2007. “Petraeus Hearts Milblogs.” *Wired,* 15 May, <www.wired.com/dangerroom/2007/05/petraeus_hearts/#ixzz0lPYrKSUg>.

Shane, Scott. 2011. “Spotlight Again Falls on Web Tools and Change.” *New York Times,* 29 January, <www.nytimes.com/2011/01/30/weekinreview/30shane.html?_r=1&ref=scottshane>.

Sipress, Alan, and Sam Diaz. 2007. “A Casualty of War: MySpace.” *Washington Post,* 15 May, <www.washingtonpost.com/wp-dyn/content/article/2007/05/14/AR2007051400112.html>.

UN Human Rights Council. 2012. *The promotion, protection and enjoyment of human rights on the Internet*. www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session20/Pages/ResDecStat.aspx.

US Department of State. No date. “21st Century Statecraft.” <www.state.gov/statecraft/overview/index.htm>.

US Department of State and USAID. No date. *The Quadrennial Diplomacy and Development Review*. Fact Sheet, Washington, DC, <www.state.gov/documents/organization/153109.pdf>.

Ward, Stephen J. A. 2011. “Social Media: Tool of Revolution or Repression?” *MediaMorals*, University of Wisconsin-Madison, 31 January, <ethics.journalism.wisc.edu/2011/01/31/social-media-tool-of-revolution-or-repression/>.

Whitelaw, Kevin. 2009. “In Today's Army, the GI Diary is Written in Tweets.” *National Public Radio*, 15 September, <www.npr.org/templates/story/story.php?storyId=112823233>.

Willemssen, Joel C. 1995. “Information Superhighway: An Overview of Technology Challenges.” Washington, DC: US General Accounting Office, January.

Winner, Langdon. 1985. “Do Artefacts Have Politics?” In *The Social Shaping of Technology: How the Refrigerator Got Its Hum*, Donald MacKenzie and Judy Wacjman (eds.), 26-38. Philadelphia: Open University Press.