

Towards an Online Bill of Rights

Sarah Oates

There are a lot of things happening in the online sphere, but effective self-governance is not one of them. This chapter asserts that there is a need for an online ‘Bill of Rights’ and reflects on how this might be made possible for netizens. Critical areas under discussion in the Onlife manifesto include concepts such as hyper-history, the lack of mediation in the online sphere, the erosion of privacy, a loss of context, distributed epistemic responsibility and even the right to digital euthanasia. A central theme in the Onlife Manifesto is the way the ‘virtual’ and ‘real’ are now woven together into an enmeshed life experience. Yet, the way in which individual rights are understood and asserted vis-à-vis the online sphere remains remarkably unarticulated. How can we continue as humans if a key part of our daily experience takes place overlapping into a sphere in which our rights are not articulated and—even more importantly—protected? Yet, even though we have arrived at what Ess has called in a discussion of the Onlife Manifesto a “critical moment” for policy intervention regarding our digital future, it would seem paradoxically that the online sphere itself lacks this capability to inspire or create policy to protect online citizens.

This chapter addresses the issue of online awareness of internet rights and policy on three levels. First, it reflects on why there is a lack of effective self-governance and policy direction in the online sphere. This calls for an explanation of how people perceive the norms of the online sphere—and how some utopian perceptions may cloud judgments about the increasingly asymmetric power relationships among online users, internet-service providers and the state. Secondly, the chapter mines some of key points raised in the Onlife project, as well as those identified in other calls for online rights, to suggest a list of six fundamental online rights to demand: the right to privacy, the right to own your own data, the right to a personal life, the right to avoid being forced offline for safety, the ability to switch off when needed as well as public spaces for civic debate online. Finally, this chapter discusses the difficult issue of translating crowd-sourced discussion into actual policy. It is not surprising that new technologies call for new governance, but as the internet has

S. Oates (✉)

Philip Merrill College of Journalism, University of Maryland,
College Park, USA

e-mail: soates@umd.edu

changed people, technology and their affordances simultaneously at great speed, the linked issues of self-awareness and self-governance in the online sphere are critical. How can we possibly unlock the potential of self-aware, online governance? The answer may lay in a greater effort by state Leviathans such as the European Commission. Overall, it is more useful to stop dreaming of cyber-utopias and start creating cyber-preserves of free exchange.

1 The Lingering Myth of Cyber-Utopianism

There is an astonishing gap between how people perceive internet ‘freedom’ and the realities of the digital sphere in the 21st century. The mistaken conviction that the internet is both unfettered by the norms of capitalism and can bring fundamental political change to the globe is not surprising. The internet was fostered by an unprecedented amount of social capital as well as has created unique ways for humans to interact. In the face of some grim realities about the way in which the digital world tends to reinforce the political and economic status quo, people still broadly ascribe open and disinterested roles to this communication sphere. It is possible that the internet still can provide the type of support to human capital that was present to a large degree in its early days within the research community. However, if we do not acknowledge that the digital world has become largely colonized by market and political forces, then it will be too late to preserve the essential social value of the internet. It is important to articulate what is unique and important about being human in the digital age—and how the central positive aspects can be preserved in the interests of the citizens, rather than for the demands of states or corporations. This led the Onlife initiative to attempt to articulate the key challenges to promote and protect citizen interests in the digital era.

An examination of various ‘manifestoes’ and other documents that articulate rights (and responsibilities) in the online sphere show a wide range of norms and ideals (see Table 1 for a sample list). However, a conviction that resonates through many of these declarations is the idea that the internet can fundamentally change how humans (and, by association, states) relate to one another. For example, Dyson et al.’s *Cyberspace and the American Dream* states that the “powers of mind are everywhere ascendant over the brute force of things” and implies that this is a shift in power away from traditional political institutions: “It also spells the death of the central institutional paradigm of modern life, the bureaucratic organization. (Governments, including the American government, are the last great redoubt of bureaucratic power on the face of the planet, and for them the coming change will be profound and probably traumatic.)” Even more striking is John Barlow’s *A Declaration of the Independence of Cyberspace* (1996), which identifies the internet as a completely new and different way of being human: “I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.” The identification of the idea of ‘sovereignty’ is very useful, in that in many cases people are declaring that the norms of the internet are something new and different that transcend sovereignty and laws, some ‘hacker’ manifestoes going so far as to

Table 1 List of manifestoes and declarations relating to online sphere (alphabetical order, date of initial publication listed where available)

10 Internet Rights and Principles Internet Rights & Principles Coalition http://internetrighsandprinciples.org/site/wp-content/uploads/2011/09/irp3.jpg
A Crowd-sourced Declaration of Rights Source: Reddit Sub-Group http://www.reddit.com/r/fia/comments/vuj37/digital_bill_of_rights_1st_draft/
A Declaration of the Independence of Cyberspace Source: John Perry Barlow, 1996 https://projects.eff.org/~barlow/Declaration-Final.html
A Digital Citizen's Bill of Rights Source: Keep the Web Open http://keepthewebopen.com/digital-bill-of-rights
A Hacker Manifesto By Par McKenzie Wark Published 2004 by Harvard University Press http://subsol.c3.hu/subsol_2/contributors0/warktext.html
CATO Institute: The Libertarian Vision for Telecom and High-Technology By Adam D. Thierer and Clyde Wayne Crews Jr. http://www.cato.org/publications/techknowledge/libertarian-vision-telecom-hightechnology
Cyberspace and the American Dream: A Magna Carta for the Knowledge Age By Esther Dyson, George Gilder, George Keyworth and Alvin Toffler Future Insight Release 1.2, August 1994 http://www.pff.org/issues-pubs/futureinsights/fi1.2magnacarta.html
Declaration of Internet Freedom (1) http://www.internetdeclaration.org/
Don't Make Me Steal It Digital Media Consumption Manifesto http://www.dontmakemesteal.com/en/
Draft Code of Ethics for the Information Society Source: UNESCO http://unesdoc.unesco.org/images/0018/001871/187196e.pdf
Internet Manifesto How journalism works today. Seventeen declarations, 2009 http://www.internet-manifesto.org/
Manifesto for Agile Software Development http://agilemanifesto.org/
Principles on Freedom of Expression and Privacy By Global Network Initiative http://www.globalnetworkinitiative.org/principles/index.php
The Cluetrain Manifesto By Rick Levine, Christopher Locke, Doc Searls and David Weinberger, 1999 http://en.wikipedia.org/wiki/The_Cluetrain_Manifesto http://cluetrain.com/
THE:CYBER COM/MUNIST: MANIFESTO By Richard Barbrook, 2007 http://www.imaginaryfutures.net/2007/04/18/by-richard-barbrook/
The Euston Manifesto http://eustonmanifesto.org/the-euston-manifesto/

Table 1 (continued)

The Hacker Manifesto

Source: + + + The Mentor + + +

Written January 8, 1986

<http://www.mithral.com/~beberg/manifesto.html>

The Mozilla Manifesto 2012

<http://www.mozilla.org/about/manifesto.en.html>

Rights and Obligations

Source: Commission nationale de l'informatique et des libertés (CNIL)

<http://www.cnil.fr/english/the-cnil/rights-and-obligations/>

UN Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue

http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

We the Web Kids

By Piotr Czerski

<http://www.theatlantic.com/technology/archive/2012/02/we-the-webkids/253382/>

Note: This list is meant to be a useful sample rather than encyclopaedic. It was compiled initially by Nicole Zwaaneveld for the Onlife Initiative

redefine a ‘hacker’ as someone who is reconfiguring not just code, but society itself. Overall, Barlow’s comment that “the challenge is as daunting as the opportunity is great” is compelling. The unique properties of the internet—the ability to transcend national borders, to create content with virtually no economic barriers, to communicate instantaneously, for many-to-many networking—indeed do create great opportunity. But what opportunity and for whom?

Cyber-utopism suggests that property and sovereignty are irrelevant because the power of networked communication will transcend these two pillars of modern Western society. The assumption in early cyber-utopism is that the opportunity will be for the citizens to have greater power. Yet, it was not clear how the online sphere would either appropriate that power or utilize it outside of traditional political institutions such as political parties, legislatures, military forces, traditional mass media, or indeed the framework of states themselves. Evidence suggests that state policy as well as national cultural norms divide and shape the internet into a reflection of individual countries. Thus, rather than transcending state boundaries, the internet can be seen to reinforce state boundaries and powers (Oates 2011). If the cyber-world is indeed an other, utopian sphere than it is precisely that—an alternative sphere that is devoid of the true institutions of power, a place for people to network and collaborate but ultimately only a landscape of ideas. The paradox is that if the online sphere remains ‘pure’ and above traditional political institutions, it also remains relatively powerless and irrelevant in modern political life. Thus, while the online sphere was perceived to be outside of mainstream society, it remained unfettered by the powerful interests of states and markets. As corporate interests began to emerge and quickly dominate the internet (Hindman 2008), there was little protection for a fragile eco-system that relied on norms of communal sharing in which capitalistic norms of profit were not present. Cyber-liberation arguments cited in various declarations and manifestoes

(see Table 1) cling to the idea that the online sphere is entitled to different rules and regulations, particularly in terms of distribution of copyrighted material. While they may have a point that the price of goods such as music, films and books remains disproportionately high now that the cost of distribution is relatively low, the argument that the internet is a zone excluded from regular legal oversight becomes increasingly weaker as the online and offline worlds continue to converge.

Interestingly, the *We the Web Kids* declaration by Piotr Czerski argues that there is no resonance to the idea of a ‘virtual’ world as young people of his generation seamlessly integrate information communication technologies into their daily lives. *We the Web Kids* makes this point in relation more to the social habits of the younger generation, but it’s a valid point throughout society as the web is “not something external to reality but a part of it: an invisible yet constantly present layer intertwined with the physical environment ... The Web is a process, happening continuously and continuously transforming before our eyes; with us and through us. Technologies appear and then dissolve in the peripheries, websites are built, they bloom and then pass away, but the Web continues, because we are the Web; we, communicating with one another in a way that comes naturally to us, more intense and more efficient than ever before in the history of mankind.” Thus, it is no longer useful to talk about the internet as though it were a separate universe. It is interwoven with human existence, with all the affordances and drawbacks this may bring. Czerski then tries to argue that as popular culture is part of this collective consciousness, it is unfair to claim copyright over things such as popular music television shows and movies. Yet, it is precisely *because* the online and ‘real’ words have now merged (as Czerski himself argued earlier in the piece) that gives weight to the argument that historic rules of ownership and copyright should apply to digital forms of creative output.

While acknowledging the origins of the internet as particularly collaborative and detached from economic or national concerns, it also must be recognized that the world has moved on. Yet, has the common conception about humanity’s relationship to the online sphere really moved on? The lingering conviction that the rules are different for online rather the ‘real’ spheres continues, as people continue to interact in ways online that they would never do in their daily, non-internet lives. On the one hand, this spawns stories about a Congressman sending sexually suggestive photos via social networking or the viral distribution of an expletive-laden email from a sorority member upset that her sisters weren’t friendly enough to male visitors at a social event.¹ On the other hand, it gives people a false sense of security when they engage in the online sphere. The problem is not so much people engaging in socially unappealing behaviour, being duped by email fraud or having their accounts hacked by online viruses so that their personal details can be stolen. More significantly, the assumption that the internet provides a safe, ‘other’ sphere blinds online users to their vulnerability to data aggregators (Solove 2004) working for corporations, security services or even simply criminals. Most internet users are unaware of the depth and breadth of personal information that is created via routine

¹ Former Congressman and failed New York City Mayoral Candidate Anthony Weiner and Rebecca Martinson of the Delta Gamma chapter at the University of Maryland.

online interactions—including but not limited to search, email on many platforms, uploading photographs, clicking on websites, buying products—that are harvested by companies and sometimes state security officials. We are leaving tracks all over the online world, the impact of which is discussed by other authors of the *Onlife Manifesto*. The point that is emphasized here, however, is that there is a considerable gap between what people perceive is being revealed about themselves and the massive, detailed and mostly permanent data trails that they leave behind.

2 Towards a European Onlife Bill of Rights?

European citizens live in a ‘fog of data’ in the digital age. On the one hand, the digital age augments life by giving individuals direct access to information and networks that previously were limited by physical or practical barriers. On the other hand, as Broadbent and Lobet-Maris write in their chapter, the advent of the digital age has eroded barriers between individual and self in new and challenging ways. In practical terms, this raises concerns about data and identity theft. In more philosophical terms, this means significant challenges for people in negotiating a balance between different aspects of what it means to be human. In particular, this raises problems in terms of preserving different levels of privacy as the digital presence merges various identities—including student, teacher, worker, lover, child, sibling, parent, etc.—into a single visible entity. As Broadbent and Lobet-Maris write, “The individual is always visible and transparent, open to the view of all.” This creates enormous stress on individuals, in particular due to the lack of “unclear social norms and regulations.”

But does it have to be this way? Without getting bogged down in a philosophical discussion of the power of technology versus the will of Man, it is possible to set out tenets that can help individuals to negotiate the digital landscape. In some ways, these can parallel how society negotiates issues surrounding information in society in general. While the digital age brings challenges in new forms, the questions for humankind are essentially the same when we discuss defining the limits between the personal and the public. The problem is that these issues are not being discussed in a meaningful way. People are heavily engaged in commerce and entertainment in the online sphere, but there is a dearth of self-aware political discussion and mobilization about the very communication environment that dominates the 21st century.

What we are left with is a lack of online cultural norms that can lead individuals astray if they continue to perceive the online sphere as free from norms—or even laws—that often have surprisingly harsh consequences. The way in which a false sense of security can lead people astray in a social sense is primarily anecdotal. One of the highest profile cases was that of former U.S. Representative Anthony Weiner, who resigned his seat in 2011 after admitting to sending a sexually suggestive picture of himself via social networking.² Indeed, he even failed to learn from this

² For background, see <http://abcnews.go.com/Politics/rep-anthony-weiner-picture/story?id=13774605>, (last accessed September 28, 2013) and <http://www.myfoxchicago.com/story/22919644/anthony-wein->

experience and admitted to more of this behavior during his unsuccessful bid to run on the Democratic ticket for Mayor of New York City in 2013. While this incident underlines the ability of the internet to identify inappropriate behavior by public figures, it also shows how even a U.S. congressman—arguably a fairly intelligent and media savvy individual—would still cling to the idea that the internet was somehow exempt from surveillance, taste or appropriate behaviour. The troubling case of Weiner aside, U.S. politicians in particular have been found that any traditional tolerance of ‘offline’ behaviour has disappeared, with the online Drudge Report responsible for breaking the Monica Lewinsky/President Clinton scandal, the damage to Senator Trent Lott’s career when a tape of his praise of a racist politician was broadcast online, and, more recently the release of a video tape during the 2012 U.S. Presidential elections in which Republican candidate Mitt Romney dismissed 47% of Americans as “dependent on the government” and failing to “take personal responsibility and care for their lives.”³

If knowledgeable politicians are falling victim to the open nature of communication online, what about average citizens? There is rising evidence that online profiles are used to judge people, not merely socially but by key gatekeepers such as employers or university admission staff. A survey of more than 2,000 hiring managers and human resource professionals in the United States in 2012 found that 37% of companies used social networking sites to research job candidates and another 11% said they planned to start the practice.⁴ About a third of the companies who researched candidates on social media found that the information caused them not to hire a candidate, including when they found provocative or inappropriate photos; information about the job candidate drinking or using drugs; or evidence that the candidate had poor communication skills. By the same token, almost as many managers (29%) reported that they found something positive about job candidates in their social-media records (personality, background, professional image, good communication skills, good range of interests, creativity, positive comments from others). Interestingly, 15% of the companies interviewed banned the practice of using social media to research job candidates, showing that there is a deep division in perceptions of online privacy even amongst U.S. employment managers.

Although universities in the United States are more likely to use social media in an attempt to attract students rather than to vet applicants to their programs, it is a two-way street, according to a survey by Kaplan Test Prep in 2012.⁵ A survey

er-caught-in-another-sex-scandal-wife-sticks-by-him (last accessed September 28, 2013).

³ See text at <https://historymusings.wordpress.com/2012/09/19/full-text-campaign-buzz-september-19-2012-mitt-romneys-47-percent-victim-voters-speech-at-may-private-fundraiser-mother-jones-video-transcript/> (last accessed September 28, 2013).

⁴ The survey was conducted online with the United States by Harris Interactive on behalf of CareerBuilder (careerbuilder.com) with 2,303 hiring managers and human resource professionals between February 9 and March 2, 2012. Report online at <http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr691&sd=4%2F18%2F2012&ed=4%2F18%2F2099> (last accessed September 28, 2013).

⁵ For the 2012 survey, 350 admissions officers from the nation’s top 500 colleges and universities—as compiled from U.S. News & World Report and Barron’s—were polled by telephone between

of college admissions officers found that schools are “increasingly discovering information on Facebook and Google that negatively impact applicants’ acceptance chances.” While the survey found only slight growth in the percentage of admissions officers who checked Google (27%) and Facebook (26%), the admissions officers were getting much better at finding bad things: The percentage of admissions officers who said they discovered something that “negatively impacted” an applicant’s chances of getting into the school nearly tripled from 12% in 2011 to 35% in 2012. The admissions officers were unhappy with evidence of plagiarism, vulgarities in blogs, alcohol consumption in photos, things that made them “wonder” and “illegal activities,” according to the study. Indeed the comments about the finding from a Kaplan official reflect many of the concerns raised in the Onlife Manifesto: “Additionally, we’re seeing a growing cultural ubiquity in social media use, plus a generation that’s grown up with a very fluid sense of privacy norms. In the face of all these trends, the rise in discovery of digital dirty laundry is inevitable,” said Jeff Olson, Vice President of Data Science, Kaplan Test Prep. “With regard to college admissions, the traditional application—the essays, the letters of recommendation—represent the polished version of an applicant, while often what’s found online is a rawer version of that applicant. Schools are philosophically divided on whether an applicant’s digital trail is fair game, and the majority of admissions officers do not look beyond the submitted application, but our advice to students is to think first, Tweet later.” Echoing the problem of a lack of norms for employers, Kaplan’s survey found that only 15% of the college admissions offices surveyed even had rules regarding the checking of applicants’ social networking content.

What emerges from these examples is a lack of consistent practices as to whether the internet is considered a public or private space by employers and admissions officers in the United States. Coupled with the confusion by individuals—and the continuing list of people who are reported in the mass media as ‘caught out’ via internet content despite significant evidence that nothing can be considered private in social media. While these examples are from the United States, the issues are global because countries all over the world lack strong laws or even norms in these areas. As a result, we need to consider how to articulate a set of norms and values for a new communication era—and these norms should be articulated rather than left to chance. It isn’t useful or fair to leave negotiating the evolving digital landscape to the individual. In part, this is structural as corporations and governments have, so far, been more effective at harvesting information than protecting the rights of individuals. This is unsurprising given that the logic of both capitalism and state power dictate that the needs of corporations or the state would outweigh the needs of individual consumers or citizens. In addition—and this is a more subtle and less discussed point—individuals are vulnerable to a range of factors in the digital age that are linked to the very affordances of the digital world that people cherish and embrace. Broadbent and Lobet-Maris define this (in part)

July and September 2012. See <http://press.kaptest.com/press-releases/kaplan-test-prep-survey-finds-that-college-admissions-officers-discovery-of-online-material-damaging-to-applicants-nearly-triples-in-a-year>.

within the frame of attention. Attention has become ‘monetized’ so that we are constantly playing the dual role as attention-consumer and attention-attractor in order to maintain or promote our place in life. Yet, there is more to being human in the digital age than a sort of meter that monitors the amount of attention we can attract in a crowded digital sphere. We should not be reduced to our online rating, as measured through our number of Facebook friends, Twitter followers, position in the Googlearchy, etc. Individuals need to recognize that they should have agency and choice in the online sphere and that they should have structures in place to support this agency and choice.

3 A Digital ‘Bill of Rights’

How can we articulate these thoughts into principles for policy? The following ideas were developed during the Onlife meetings from discussions at the first workshops. Much of the work of the Onlife Manifesto is dedicated to identifying core issues; while certainly not encyclopedic the six points below are an attempt to identify the core issues. In addition, they resonate with a range of declarations developed regarding rights and the online sphere as listed in Table 1.

1. Everyone has the right to privacy.

When attention is monetized through the constant harvesting of online personal activity and data, we lose privacy (Cohen 2012; Solove 2004). When states chose to monitor citizens in the online sphere, we lose privacy. When technology fails to keep its promise of anonymity, we lose privacy (Ohm 2009). The ongoing argument to support the harvesting of personal data has been that it is a contract between the internet-service provider and the individual, i.e. if you use Google or Facebook, you are allowing your data to be tracked in order to use the service. States use a variety of arguments to support harvesting online information (either openly or covertly), ranging from a need to better respond to citizens to anti-terrorism efforts. There are two fundamental problems with this ‘contract.’ First, there is evidence that ISPs as well as governments have not been clear with consumers or citizens about the way in which the data is tracked and used, creating a digital profile for users. It might be more useful to think of this as a sort of digital ‘tattoo’ or what Solove (2004) called a “digital dossier” because of its permanence. Secondly, there is a widespread lack of individual awareness of how the private becomes permanently public in the digital age, which is reflected in the way in which people post information, images, video, etc. that are damaging to themselves and others. In this way, individuals create permanent profiles of themselves that they cannot delete (or refute).

There is a slightly more compelling argument that the state should be able to react to obvious threats to state security that are visible in the online sphere. However, as a U.S. Supreme Court justice once said, freedom of speech should only end when you stand up and yell ‘fire’ in a crowded theatre, i.e. you should only lose the right to free discourse if you are creating a clear and present dan-

ger.⁶ There should be a defined limit or test for what is state security risk and what is acceptable radicalized discourse in the online sphere. While this is a part of a wider debate about the state, the public and information in the post 9/11 world, the harvesting of online data so radically realigns the power relationship between the harvester and the subjects that this debate becomes much more pressing and urgent. It also would appear that governments lack the self-restraint not to monitor a wide swathe of citizens in the name of national security. The revelation in June 2013 that the National Security Agency in the United States was tracking huge tranches of mobile phone records drew attention and debate from Americans about government surveillance, but the more critical issue of the potential to track citizen behavior via the online sphere at a far more granular level still does not seem to be understood by citizens.

2. Individuals own their own data.

This is a bold statement, in that the business model of many ISPs is based on the harvesting and sale of data to advertisers. This is not to suggest that ISPs could be stopped from collecting individual data, but the idea of the right to one's data should be considerably strengthened. While many people easily recognize that information that they enter into a computer (such as names, dates of birth, bank account numbers) is data that needs to be protected, there is far less awareness of the more subtle and personalized data patterns, essentially digital fingerprints, that are created by individuals in their daily internet interactions (particularly search behaviour). There can be two views here that are compatible within the idea that individuals own their own data and the public own public data. In a cooperative move with ISPs, the data can be shared. For example, Google makes public a great deal of its aggregate data via Google Analytics in an attempt to show the value of search data in informing economic, social and political life. However, Google does not make its data archive linked to individuals public unless forced to do so by national laws—and as shown by its withdrawal from China, Google will resist this where possible. (However, the NSA scandal suggests that Google may be compelled to share data on individuals more frequently than they are able to report.) In a more pro-active approach, society can choose to block or severely limit the way in which individuals are monitored by ISPs. European states have moved in this direction recently by requiring ISPs to inform users about cookies and having users 'opt in' instead of 'opt out'. The notion of informed consent imposed by law is an important and useful direction.

3. Everyone has a right to a personal life.

This is linked to the issue of privacy as discussed above, but it is somewhat different. No one should have to friend on line a teacher, student, co-worker, client, etc. There should be clear delineation between what is an online business/education tool and what is a social/personal tool. Part of this is an issue of ISP design. Facebook, created by U.S. college students, is based on the American ideal of networking in which personal and professional relationships are encouraged to merge. However, as has so often been the case with online interfaces, the sheer scale and scope of Facebook has intensified this relationship in unhelp-

⁶ See the U.S. Supreme Court decision in *Scheck v. United States*, 1919.

ful ways (coupled with the toxic need for attention that drives many people to compulsively post minute information about their personal lives on line). It has created the ‘perfect storm’ to erode the boundaries between the personal and professional.

4. No one should have to switch off completely to protect himself or herself. Here the argument (particularly from the older generation) is that one can simply opt out of social networking or the online sphere in general. This is almost impossible for much of the population. For example, students clearly use social networking to communicate with their peers at school and manage relationships. The level of enthusiasm for it varies, but it is not really optional. A college student who is not on Facebook (or the current dominant social network in his or her environment) would be socially and academically isolated, missing the communication and even links to critical information for study. Broadbent and Lobet-Maris also are correct to point out that a new digital divide emerges when management can remain online throughout a working day and workers cannot. This is the new type of digital divide that warrants attention and concern. The issue of the timing and control of access should be considered in more depth.
5. Switching off sometimes should be encouraged—and cultivated. As noted in meetings of the Onlife project, the internet has become a sort of external brain for a lot of people. It has the ability to stimulate and delight through access to information and people, supporting us in our quest to be better informed as well as through enriching relationships. However, this is where the point made about attention by Broadbent and Lobet-Maris is so important. We need to cultivate the ability to pay attention and concentrate, as it is becoming a lost art. This type of focused attention is still necessary, in particular for learning and close relationships. Perhaps it is not so much about ‘switching off’ as withdrawing from the public to private, as discussed in earlier points.
6. There should be ‘third spaces’ that are owned and regulated by the European public. Again, here we have an issue in which the U.S. model of communication has come to dominate in Europe and it does not really fit. In particular, Facebook operates under the U.S. libertarian system, in which there is little distinction among the commercial, the private and the state in terms of information production and dissemination. Americans reject the notion of the state as the instrument of social and political change; rather, they view the state as the handmaiden of the wishes of the public. While there is a lot of evidence that the U.S. state is bigger, more powerful and more redistributive than the common American believes it to be, it also means that Americans are quite comfortable with the fusion of commercial and political power in the information sphere. The same is not true of Europeans. European countries have created either public or state broadcasting systems, as well as tend to have a greater emphasis on the state’s role in inculcating public debate. This means that U.S.-designed internet interfaces and norms of data openness are not appropriate. It suggests that European states and the European Union itself need to be more pro-active in creating a public ‘agora’ in which citizens can debate and discuss political ideas in a less polarized way, as well as in a way that is more supportive of European democracy at the national or Union level.

Here, one could reflect on some evidence surrounding political debate, parties and elections in the United States. As Richard Davis (2009) points out in his study of U.S. political blogs, influential blogs in the United States are partisan. They reflect the divide between Democrats and Republican, who are typically more at odds over social values than economic issues. Despite this polarity—or perhaps because of it—blogs are a particularly vibrant part of the U.S. news discussion, often quoted or breaking political stories in their own right. Online news sources have become popular, not just as elite influencers, but as news outlets themselves. Thus, the United States has more developed, if at times polarized, online political discourse than European countries such as the United Kingdom. The question remains whether this is one of culture or—as Scott Wright would argue—one of design. Wright, who has studied the effect of different online formats on the nature of discussion, argues that online deliberation can be ‘engineered’ by particular web interfaces (2012). Left to chance or merely the market, these deliberative spaces do not arise. This is in part because political interaction and discussion form only a very small part of what people do on line. However, Wright’s research has found that when given opportunity and motivation, people are ready and willing to discuss political issues and mobilize on line in the United Kingdom.

The idea of an engineered online ‘agora’ is particularly important during a period of crisis. My own research and that of others has found that online discussion becomes more intense—and much more closely linked to offline manifestations ranging from elections to protests—in times of political crisis (Khamis and Vaughn 2012; Lewiński and Mohammed 2012; Oates 2013). As the Euro crisis comes to a head in Europe, where is the common space for Europeans—as opposed to citizens of individual nations—to discuss and debate these issues in a rational, informed manner? At an even more fundamental level, where is the common space in which authoritative information about debt, taxation, fairness, rules and consequences can be exchanged among a European public? The current coverage of the Euro crisis is, unsurprisingly, framed through the lens of national media. As a result, the public are woefully uninformed—and even misinformed—about the information and issues at stake. As in any disputed, nationalistic information sphere (reflect on audience issues in Northern Ireland or the former Yugoslavia), there is no real accepted reality. As a result, it is enormously difficult to discuss the issue in a ‘European’ way. The internet could provide such common space, yet does not at this time.

4 From Creative Commons to Civilized Commons

Social scientists often think in opposing dualities—voters versus non-voters, communists versus capitalists, citizens versus elites, war versus peace. We present a worldview in this way in order to stimulate debate, although within various

epistemic communities the more useful debates often deal with the shades of gray. For example, it is not as if there are vast crowds of citizens wandering about under the whip hand of a circle of elite leaders (although Left publications might put forth this case). Rather, as members of a society, there are times when we contribute and times when we simply consume, not really fulfilling the Leninist idea of ‘from each according to his abilities, to each according to his needs’ but rather in the less economical and less elegant way of taking on shifting roles of responsibilities and benefits. Thus, change is better understood as evolution rather than revolution. However, there has been a lot of talk about internet ‘revolutions’, whether it is the ‘Twitter Revolution’ in Iran in 2009 or the ‘Facebook Revolution’ in Egypt in 2011. While many of the manifestoes discussed above (especially Barlow’s) describe the internet in revolutionary terms vis-à-vis power redistribution from existing elites to the masses, the twin forces of national power and commercial online dominance make that unlikely.

Yet, there are enough elements of the initial forces that shaped the internet to make it a social tool that is unlike anything that has come before. An overlooked element of the internet is speed. Its ability to communicate instantly among many without national or corporate frames is indeed revolutionary. In this particular way, the internet rebalances power between elites and masses. So far, this dynamic has been more about challenging political elites than replacing them, as the experience in Egypt suggests. While states are learning to harvest the online world to better understand and/or control their citizens, traditional political institutions are not well designed to take full advantage of the social capital offered by the online sphere. Rather, it may ultimately emerge that distributed power networks become more authoritative—and hopefully more effective—at spreading democracy than established power institutions. The articulation of the rights (and responsibilities) of online citizens is a first step in preserving the potential of the online sphere to improve the condition of Man.

There is an element to the Onlife Manifesto that is revolutionary and this is implicit in both the manifesto itself and the recent reflection from Charles Ess for the Onlife initiative: Governments cannot be passive in the face of evolving technology. Ess, in his chapter, usefully points to the historical evidence that businesses do not automatically safeguard consumers when they introduce new technology (his example of the exploding steam engines was particularly evocative). While this is regrettable, it is also understandable under the logic of the market. No single company could simultaneously bear the cost of innovation and public safety, particularly with the introduction of new technology. The problem is that the internet was supposed to be different; it was supposed to be a post-modern collaborative effort that was above the demands of both sovereignty and capitalism. That may have been true in the initial stages, but for the past decade there has been ample evidence that the internet is the prime locus for business (Google, Facebook, etc.) and national controls (as evidenced by Syria switching off the internet in late 2012 or the broader issue of how security services in nations around the globe mine the internet to monitor citizens). The notion that the internet does not have profound economic and politi-

cal power in the traditional sense is absurd, yet the clear vision of this is blurred by a hazy memory of ‘cyber-utopia’ as embraced by Tim Berners-Lee et al.⁷

The problem is that the debate about the benefits and drawbacks (a crude duality) of the online sphere has not followed lessons of history, perhaps because there has been too much comparison of the internet to the traditional mass media. While the internet shares many of the same issues as the traditional media (such as journalistic ethics, news values, serving as propaganda in times of war and the problem of ‘dumbing down’ the news), the online sphere offers many additional, distinctive opportunities and threats to society. These are articulated in the Onlife Manifesto, but the next step is to express more forcefully what we mean in all of this: The state needs to play a role. What role, given that we have established that this is not about relatively straightforward issues such as access or protecting children (although those are specific concerns within a much broader discussion)? The Onlife Manifesto shows that there is a need for the choices and tradeoffs in the online sphere to be made more evident. That is to say, people need not just connection to the internet or even engagement in the online sphere; they need informed engagement on a relatively level playing field that has been engineered to prioritize the rights of citizens over the needs of elites.

On the one hand, this means a focus on more nuanced and useful information for people of all generations and all socio-economic categories in Europe about both the benefits and trade-offs in engaging in the online sphere. Language about risks is not useful, particularly when there is no way for individuals to really understand, much less negotiate, risks such as loss of privacy and identity. At the same time, governments need to establish guidelines for internet-service providers such as Google, Facebook, Twitter, etc. so that people who chose to use these services are aware of data-mining the surrendering of ownership of their images and words. Overall, the risks and responsibilities need to be redistributed from lying primarily with the citizen-user and to be much more substantially shared by internet-service providers. For this exercise, we are discussing the European Union, but in many ways this is the role of national governments as well. So out of all this comes again this idea of the pairing of rights and responsibilities, with perhaps a parallel to motor-ing privileges. Just as citizens are responsible for safe driving, governments are responsible for eliminating hazards from the motorways. Citizens have the right to participate in the online sphere, but they have the responsibility to learn how to navigate it to protect themselves (and others). At the same time, governments have the responsibility to protect citizens against dangerous technology, such as that which allows excessive data mining and loss of privacy rights. If governments can

⁷ Ironically, the development of key points of the internet—such as packet-switching, TCP/IP, the concept of Email, the World Wide Web and web browsers—would never have been developed without the early, open and collaborative nature of the internet that paralleled the heavy involvement of academics and did not follow the laws of market capitalism. However, commerce and nation-states have long since expropriated this free-ware capital, a move that is perhaps so painful to early web developers that it seems under acknowledged. Certainly, there are elements of the online sphere that both spread and foster values of disinterested participation, but they are now the exception rather than the rule.

foster the creative spark and the potential that brought the internet so far into our daily lives at such a rapid pace, then it can help preserve (rather than destroy) the most promising way to unlock human potential on our planet. Manifestoes, ranging from the Magna Carta to the Declaration of the Independence to the Communist Manifesto, delineate fundamental shifts in the relationship between elites and rulers. We are at a crossroads in terms of the power balance between citizens and elites/powerless and powerful in the digital world; the Onlife Initiative seeks to make visible these issues and forces.

Open Access This chapter is distributed under the terms of the Creative Commons Attribution Noncommercial License, which permits any noncommercial use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.

References

- Cohen, J. E. 2012. *Configuring the networked self: Law, code, and the play of everyday practice*. Connecticut: Yale University Press.
- Davis, R. 2009. *Typing politics: The role of blogs in American politics*. New York: Cambridge University Press.
- Hindman, M. 2008. *The Myth of Digital Democracy*. Princeton, N.J.: Princeton University Press.
- Khamis, S., K. Vaughn. 2012. We are all Khaled Said: The potentials and limitations of cyberactivism in triggering public mobilization and promoting political change. *Journal of Arab & Muslim Media Research* 4 (2–3): 145–163.
- Lewiński, M., D. Mohammed. 2012. Deliberate design or unintended consequences: The argumentative uses of facebook during the Arab spring. *Journal of Public Deliberation* 8 (1): 1–11.
- Oates, S. 2011. Going native: The value in reconceptualizing international internet service providers as domestic media outlets. *Philosophy & Technology* 24 (4): 391–409.
- Oates, S. 2013. *Revolution stalled: The political limits of the internet in the Post-Soviet sphere*. New York: Oxford University Press.
- Ohm, P. 2009. Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review* 57, p. 1701. University of Colorado Law Legal Studies Research Paper No. 9–12. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006. Accessed 18 June 2013.
- Solove, D. J. 2004. *The digital person: Technology and privacy in the information age*. New York: New York University Press.
- Wright, S. 2012. Politics as usual? Revolution, normalization and a new agenda for online deliberation. *New Media and Society* 14 (2): 244–261.