The Internet and the State:
A Survey of Key Developments

The Internet and the State: A Survey of Key Developments

Michel van Eeten, Milton Mueller and Nico van Eijk

RAAD VOOR
MAATSCHAPPELIJKE
ONTWIKKELING

De Raad voor Maatschappelijke Ontwikkeling is de adviesraad van de regering en het parlement op het terrein van participatie van burgers en stabiliteit van de samenleving. De RMO werkt aan nieuwe concepten voor de aanpak van sociale vraagstukken.

De Raad bestaat uit onafhankelijke kroonleden: de heer mr. S. Harchaoui (voorzitter), de heer drs. B.J. Drenth, de heer prof. dr. P.H.A. Frissen, de heer dr. E. Gerritsen, mevrouw drs. J.G. Manshanden MPA, de heer prof. dr. L.C.P.M. Meijs en mevrouw prof. dr. I. van Staveren. De heer dr. R. Janssens is algemeen secretaris van de Raad.

Raad voor Maatschappelijke Ontwikkeling
Rijnstraat 50
Postbus 16139
2500 BC Den Haag
Tel. 070 340 52 94
www.adviesorgaan-rmo.nl
rmo@adviesorgaan-rmo.nl

NUR 740
Zet- en binnenwerk: Textcetera, Den Haag
Basisontwerp: Christoph Noordzij, Wierum

Contents

Introduction

This paper sets out to provide a concise overview of key developments in relation to Internet-based services that may have an impact on public policies and ultimately on the state itself. It is intended to support the Netherlands Council for Societal Development (*Raad voor Maatschappelijke Ontwikkeling*, RMO) in preparing its advisory report to the Dutch government on how to deal with the impact of the Internet on society and the state.

By its very nature, an endeavour such as this – very broad in scope, very concise in description – has to be modest in its claims. We were tasked with capturing the latest thinking on these issues, grounded in the most recent academic research, without attempting a comprehensive review of the literature. Rather than mapping the literature using a specific perspective or theory, we followed a bottom-up approach, identifying the themes that have emerged in recent academic literature. We summarized those themes in the form of eight key developments in the Internet ecosystem which collectively give a good sense of the landscape:

- Increasing value of personal data
- Rise of new intermediaries
- Delegating governance to private actors
- Reasserting digital territories
- Emerging peer production and collective action mechanisms
- Adapting to hyper-transparency
- Establishing identification and attribution
- Securitization and militarization

The list could have been extended, of course, but to do so would have undermined the requirement of conciseness or truncated treatment of each individual topic. We should also note that it is difficult to define clear boundaries for a survey such as this. We focused on key developments in the Internet ecosystem which have recognizable societal impacts. We did not attempt to include psychological or behavioural research on how Internet use affects individuals, even though the trends we describe do seek to influence individual behaviour and some of these behavioural effects may, in turn, translate into societal changes over time.

Increasing value of personal data

A substantial part of the Internet economy is currently fuelled by a unique combination of user-generated content, professional content, social media platforms and behavioural advertising. The largest firms offer 'free' services, use of which generates rich data about users which is then leveraged to link users and advertisers. Through a process known as 'behavioural targeting', the advertising can be instantly customized as users with a certain profile are literally auctioned off to specific advertisers as they arrive at a website; or, ads tailored to their interests are displayed alongside their email messages or social media displays. In this framework, users actively volunteer large amounts of highly personal information (photos, likes, dislikes, location, etc.) and build an online social environment that they share with other users, while the providers offer free services ranging from search functions to email to chat, voice communication and storage – a classic two-sided market (Anderson & Gabszewicz, 2006).

There are some similarities, but also profound differences, between this media environment and the old world of mass media. The networks generated in this way – the links between people, products and services – provide an extremely deep and dense basis for constructing profiles that are individuated but also categorized on the basis of associative patterns (Acquisti & Gross, 2006). Instead of 'audiences' with specific demographics, we see a more dynamic formation and dissipation of clusters, many of which exhibit hyperbolic scaling properties. Unlike the advertiser-dominated world of commercial broadcasting, the data is linked to individual users and personally identifiable information. The use of mathematical network analysis techniques is being honed to sift through and utilize this data.

Social media sites are highly differentiated, and include not just the main social networking sites such as Facebook, Twitter and Google+, but also dating sites, video sharing, micro-blogging sites, and used car classifieds. The network effects of social media sites are often less global and more local

than many people assume (Zhang & Sarvary, 2011). To illustrate: networks in online gaming worlds such as World of Warcraft are heavily dominated by offline personal networks among people living in each other's geographical vicinity. The brand positioning of a site is not entirely under the control of the supplier; it depends on which users a site attracts. Economists call this 'spontaneous differentiation' (Zhang & Sarvary, 2011). Consumers can and do participate in multiple platforms (Lenhart, 2009) but due to network externalities and the build-up of large inventories of followers (or friends, etc.), users cannot easily shift from one social media platform to another if they do not like its policies or practices.

The new media, represented by social media, converge in one sense with the old media, and in another sense are 'creatively destroying' them. They are converging because the old media are linked into them and the old media producers have to develop a sustainable economic relationship with their online manifestations. They may move into, or attempt to become part of, social media platforms, or find new niches and revert to distinct, specialized functions.

One of the most dramatic impacts of social media has been on newspapers and news magazines. In the U.S., where the trend is most advanced, newspapers are going out of business or cutting back print publication. David Carr of the New York Times has claimed: "The audience that is worth $1 in print is worth a dime and sometimes a penny on the Web." However, new media analysts counter that it would be more accurate to say that the $1 that mainstream publishers used to receive from their audience is now split up into a hundred pennies; small publishers pick up a few of those pennies, while bigger new media companies such as Google and Facebook are amassing valuable data and picking up the dimes (RAND Media Group, 2013). People will gather news from a hundred sources: RSS feeds, Facebook, Twitter, Google News, etc. The massive explosion of information has created a nearly infinite pool of advertising space, which drives down the value of a generic impression.

These changes have led to debates about the sustainability of traditional journalism, with some looking for new business models and others calling for public funding. Social media and the mainstream press clearly embrace

different agendas. A Pew Center study showed that blogs shared the same lead story with traditional media in just 13 of the 49 weeks studied. Twitter was even less likely to share the traditional media agenda – the lead story matched that of the mainstream press in just four of the 29 weeks studied (Pew Center, 2012). The stories that gain traction in social media do so quickly, often within hours of initial reports, and leave quickly as well. While bloggers still rely heavily on the traditional press for their stories (and just a few concentrated major media outlets), Twitter relies on it less, and more on online sources. In this context we observe a shift towards a more functional approach to journalism. This is also in line with recent jurisprudence in this area, such as that of the European Court of Human Rights. The court consistently emphasizes the journalistic function of a (social) watchdog as such, not linking it to a specific profession or institution.

Obviously, one of the key political issues surrounding this online economy concerns privacy and confidentiality. How much of the user's data can be shielded from other users through customized settings? How extensively can the social media platform provider itself use, share or process the data? Under what conditions can law enforcement and governments gain access to the data? This represents an interesting dilemma in contrast to traditional one-way media models, where privacy – by its nature – is less of a problem. In the words of one critical observer: "The Internet interprets surveillance as sharing, and rewards it" (Morozov, 2013). Enticing people to share enables surveillance on an unprecedented scale. Use and abuse are two sides of the same coin. We will revisit this issue in more detail below.

Rise of new intermediaries

Not too long ago, a dominant prediction about the impact of the Internet was that it would cut out the 'middle men' (Whinston et al, 1997). Consumers would buy directly from producers, politicians would engage directly with citizens and artists would present their material directly to audiences. This development was called 'disintermediation', or the removal of intermediaries.

We now know that this prediction by and large missed its target. It is true that a variety of established intermediaries are in decline: record stores, for example, have been losing ground for well over a decade now. However, this is not because artists are selling directly to their audiences; rather, it is a consequence of the fact that other intermediaries have replaced the stores. Music has become an information good, rather than a business model based on physical media. As such , music can be distributed more efficiently via online music services such as the iTunes store and Spotify – and of course via the peer-to-peer networks or 'cyberlockers' that are also known for facilitating the unauthorized dissemination of copyright-protected works (Poort and Leenheer 2012). Online intermediaries can distribute much larger catalogues of content at lower cost. They are also integrated into the software running on the mobile devices that are increasingly used to consume music.

New and often powerful intermediaries have emerged all over the Internet: search engine providers, payment service providers, social network providers, access providers, hosting providers, cloud service providers, and others (OECD, 2010). Many of these markets are dominated by a very small number of firms. This is because many information services operate under what are called positive network effects and economies of scale. The value of a service like a social network increases with the number of users that converge on the same network. Also, the quality of the service goes up and the cost per unit goes down with each additional user. Google can improve its search results by looking at the clicks of its huge user base and by profiling

users across the other services it provides. A competitor does not get this feedback and has to recoup its costs over a smaller user base.

These dynamics have created intermediaries that form new concentrations of global economic power ('winner takes all'), often across different markets. This has political implications as well. The so-called 'Internet giants' – Google, Facebook, Apple, Amazon, Microsoft – all originated in the U.S. They are led from their U.S. headquarters and are therefore sensitive to U.S. political values and regulatory considerations. Furthermore, there are powerful lock-in effects that undermine the checks and balances of competitive markets by raising switching costs. If you and your friends are on Facebook, which now connects over one billion users, it is costly to switch to an alternative network if you should become uncomfortable with Facebook's privacy policies. Vertical integration – for example, between search engines, mobile device operating systems, messaging systems and cloud services – further increases switching costs. By controlling both the hardware and software of its devices, Apple makes it more difficult for its hundreds of millions of customers to move to another platform, enabling it to extract larger margins from the sales of third-party apps, while keeping apps out of the App Store that undermine its own business models, such as Google Voice, or its political profile, such the app by Pulitzer Prize-winning political cartoonist Mark Fiore. Purchased music and apps cannot always be ported from one platform to another, which further increases switching costs.

There are many more examples of the impact of these new centres of economic power. For states, this seems to be something of a double-edged sword. On the one hand, it pits them against increasingly powerful private entities which set *de facto* policies through their business models. On the other, states can also leverage the dominance of these firms for their own purposes – as evidenced by the recent PRISM controversy. A subpoena to Facebook can provide law enforcement authorities with more data about an individual than they could ever collect on their own. The forced deletion of a person from a social network has the same tremendous network effects as mentioned earlier. An order to remove content from the index of the dominant search engines or to remove a profile from a social network can quite effectively enforce censorship or exclude citizens or organizations from

the political and societal debate. The famous 'Multatuli' experiment by Bits of Freedom was one of the first tests to show how easily certain intermediaries are willing to comply with notice and take down requests. The role of intermediaries has become a constant element of concern, research, regulation and jurisprudence. In the literature, it has been argued that some of the dominant intermediaries, or their functions, could be considered as public goods (Introna and Nissenbaum, 2000). Others welcome dynamic, Schumpeterian competition and deride the idea that public utility-style regulation would ever pioneer innovative and attractive information services or platforms (Thierer, 2012).

Delegating governance to private actors

Many governmental authorities have responded to the governance challenges of globalization by delegating state-like regulatory and policymaking authority to private actors (Hall and Biersteker, 2003). This delegation is sometimes referred to as self-regulation. The complementary development is that the business models of certain firms have led them to adopt tasks that we traditionally associate with states, such as law enforcement.

States may formally delegate tasks, or they may tacitly agree with the *de facto* governance that private entities take on. The incentives for the state to accommodate such developments are varied. They may do this to overcome jurisdictional limitations on their authority, to circumvent constitutional checks or due process requirements that they find impractical, or because they are unable to keep up with the technical and operational demands of regulation (Hawkins et al, 2006). Whatever the reason, states have tacitly or formally delegated regulatory authority over important aspects of the Internet to private firms or multi-stakeholder institutions organized as private sector nonprofits (Latzer, 2007; Mueller, 2010).

One traditional example of formal delegation is ICANN, which governs the domain name system. In order to avoid the political problems and institutional burdens of negotiating a new international treaty, the U.S. government chose to delegate policy making authority over the DNS to a private nonprofit corporation (Mueller, 2002). Although its exercise of regulatory authority is sometimes supplemented by the U.S. government and it has an advisory committee of governments that looks more and more like an intergovernmental organization, ICANN governs primarily by means of private contracts with domain name registration service providers. In a similar fashion, the U.S. Commerce Department has delegated the lead role in moving towards an online identity system to a private, multi-stakeholder entity known as the Identity Ecosystem Steering Group (IDESG) (Grant, 2011).

The Internet Watch Foundation (IWF) in the UK is another example of delegation. The IWF has taken over the function of monitoring the Internet for 'potentially illegal' forms of child pornography and has also developed a blacklist of websites that it recommends should be blocked; the list can be used on a nominally voluntary basis by private-sector ISPs anywhere in the world. The INHOPE system – of which the IWF is a leading member – works according to the same methodology (Van Eijk et al 2008; see also Stol et al 2010). The Copyright Alert System (CAS) in the U.S. is another example. France created a formal governmental organization, HADOPI, with the authority to institute a system of increasingly severe penalties for Internet users suspected of copyright violation. In the U.S., on the other hand, five major private-sector ISPs entered into an MoU with trade associations of copyright-holders to institute a milder, graduated response system. Under this system, copyright-owners monitor P2P file sharing protocols and notify the ISP when they detect copyright violations. The ISP then privately notifies and warns the customer, and if the behaviour continues after six notifications the ISP may supplement the educational activities by slowing down the customer's access. European ISPs entered into negotiations with copyright-holders in an attempt to come up with a similar system, but failed to reach agreement. U.S. ISPs were equally unenthusiastic about graduated response measures but accepted the CAS after being pressured heavily by the U.S. government.

As stated earlier, the complementary development to formal delegation is the adopting of governance tasks by private actors. For example, Facebook aggressively investigates potential forms of child abuse on its network, fights scammers, dictates *de facto* privacy policies and enforces real name identity policies, to name just a few of its governance activities (Wagner, 2013; Hill, 2012). In the light of these governance activities, and the fact that its user population rivals that of China and India, the company has been referred to as 'Facebookistan' (MacKinnon, 2012), although others warn that casually equating these private services with sovereign power is a huge mistake. Facebook's self-regulatory activities are by no means unique. The Dutch site Marktplaats devotes substantial efforts to identifying fraudsters. Both firms, like many others, hire former police officers for these tasks. They try to persuade state law enforcement organizations to act by building and handing over case files with the necessary evidence to initiate

a prosecution. This is less a model of delegation than of insourcing by firms of tasks that have traditionally been performed by public institutions. Of course, firms have always done this to some extent – think of private security guards in shopping centres. That said, the delegation of governance does seem to have moved to a new level in the Internet ecosystem.

We should note that this trend is not universal. There are some areas where governments do not delegate, and this suggests that we are in a fluid situation with differing approaches across countries and regions. For example, certain segments of the market for online video services are subject either to classic broadcasting-like regulation (the European Audiovisual Media Services Directive) or fall under general or sector-specific regulation (privacy rules).

The overall effect of delegation to private actors is to replace statute law (legislation) with contractual (private) law. This kind of delegation can also be subject to abuse, as it can circumvent the procedural safeguards built into statute law. The U.S. Government was unable, for example, to charge Wikileaks with a crime, but it was able to convince or pressurize its domain name registrar, its hosting service (Amazon) and its donation support system (PayPal) to suspend Wikileaks' service, effectively shutting it off from sources of financial support. Another example is the state intervention in the Diginotar case, in which the Dutch government took over operational control of the company's certificates infrastructure by referring to its contractual relationship with Diginotar.[1] In the same case, the Dutch government persuaded Microsoft to postpone updating its browser certificates for its Dutch customers.

In recent years, European courts have developed jurisprudence emphasizing the need to keep restrictions and private enforcement in line with fundamental rights and the procedural safeguards of statute law. Measures have to meet constitutional guarantees and may not be disproportional (see

1 See: http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/wob-verzoeken/2013/03/20/wob-verzoek-juridisch-kader-overname-diginotar/wob-besluit-met-bijlagen-juridisch-kaderovername-diginotar.pdf .

for example the recent Sanoma and Telegraaf court cases)[2]. The jurisprudence compels EU Member States to have safeguards in place framing the boundaries for private alternatives.

2 European Court of Human Rights, 14 September 2010 (Application no. 38224/03); European Court of Human Rights, 22 November 2012 (Application no. 39315/06)

Reasserting digital territories

The globalized virtual space created by the Internet has challenged territory-based forms of governance, most notably the nation state. Delegation, as discussed above, is one response to this erosion of state governance. But states are not just accommodating the shift of governance to private entities. We have observed two developments where nation states are seeking to reassert their jurisdiction with regard to the Internet: by re-establishing national boundaries in the digital space and by extending jurisdiction beyond the national borders. The latter refers to the fact that attempts by states to assert their jurisdiction in cyberspace often lead to extraterritorial jurisdiction that threatens the exclusivity of sovereignty (WRR, 1998).

The companies that dominate Internet-based services typically operate at a global, or at least a multinational, scale. This is often characterized as a challenge to nation-state governance. While some argue that global networks require global governance structures, such new structures have emerged unambiguously only in areas that demand universal technical compatibility, such as the control over the root of the domain name system, Internet addressing and routing, and the development of Internet technical standards.

In other areas, especially content regulation, the lack of global governance structures and highly divergent values across different governments have led to reassertions of national borders in global services. In January 2012, for example, Twitter announced that it will respond to governmental censorship requests by filtering tweets on a country-by-country basis. The company developed the capacity to show individual tweets in some countries but block them in others, explaining that "until now, the only way we could take account of [legal censorship requests] was to remove content globally." Digital (re)territorialization allows them to "reactively withhold content from users in a specific country — while keeping it available in the rest of the world."

Somewhat ironically, as global service providers have become more established and powerful, compliance with national laws has become a routine part of their operations. Notwithstanding the global scale of their services,

these firms conduct commercial transactions (such as selling advertisements) or operate infrastructure in many countries and therefore fall under the local jurisdictions. A well-known example of these practices is the filtering that providers such as Google and Ebay were forced to adopt to disable the promotion and sale of Nazi paraphernalia.

Digital proxies of territorial boundaries can also be the product of private contracts. Streaming video services such as Netflix or Uitzending Gemist, for example, are contractually obliged by some copyright-owners to refuse service to users outside a certain geographical area. They often enforce this via IP-blocking, in effect re-creating the geographical boundary within the IPv4 address space. The forces that drive the adoption of such techniques, however, are constantly shifting. To illustrate: Sony has recently moved to abandon regional limitations in its new Playstation console. Furthermore, the European Commission has an active policy to remove national restrictions (e.g. in the field of copyright) in order to support the internal market.

When it comes to governance, territorial approaches to Internet policy can easily morph into expansive assertions of extraterritorial jurisdiction. Extraterritorial law has in the past been reserved for highly exceptional cases, such as crimes against humanity, piracy at sea or international drug trafficking. We are now seeing similar regimes emerging around the Internet. For example, a recent proposal to amend the Dutch criminal code would allow Dutch law enforcement agencies to break into systems outside the Netherlands, without going through the standard legal assistance procedures that apply between states. The U.S. approach to copyright enforcement in the failed Stop Online Piracy Act (SOPA) law effectively treated millions of foreign websites with .com, .net and .org domains, and IP addresses allocated to non-U.S. organizations, as 'domestic' for the purposes of U.S. law. Even without SOPA/PIPA, the U.S. has asserted extraterritorial jurisdiction in a number of copyright cases based on domain name registrations, most recently the takedown of MegaUpload.

Cloud computing is a new area where the dynamics of territoriality and extraterritoriality are visible. The 'cloud' is based on hardware virtualization, which in essence decouples software-based services from the physical computing infrastructure on which it runs. The infrastructure is distrib-

uted across many locations, connected by a network, and services and data are provided across these locations in an automated manner, responding to efficiency and reliability needs. This means that the precise geographical location of data and services is dynamic and often dispersed.

Cloud computing has raised all kinds of questions around legal jurisdiction. The recent controversy surrounding the U.S. PRISM programme is an example. This programme allowed the U.S. intelligence services access to all kinds of data of non-U.S. citizens who use the services of companies that are headquartered in the U.S., but whose infrastructures extend across the globe. Such access was possible even without secret surveillance programmes. Dutch legal scholars have highlighted the fact that the U.S.A. Patriot Act contains extraterritorial provisions that would allow U.S. law enforcement agencies to require global cloud service providers to provide them with data from Dutch higher education institutions (Van Hoboken, Arnbak, Van Eijk, 2013). The number of cases where these issues are at stake has been drawing more and more public attention (patient records, passport fingerprints, surveillance of data stored by providers of social networks and cloud service providers). One way in which the market is responding to these concerns is to offer 'national clouds', where the whole cloud is guaranteed to reside within a certain jurisdiction. In this way, geographical boundaries are re-emerging. When it might prove to be difficult to claim jurisdiction based on geographic definitions, new concepts of territoriality can arise. Citizenship might be one such concept that will gain importance (for example, the Maastricht Treaty created the notion of European citizenship in addition to national citizenship). States might feel the need to create additional safeguards to protect their citizens beyond national geographic borders.

There have been concerted efforts by some governments to use traditional intergovernmental means to globalize certain areas of Internet governance, such as intellectual property enforcement (e.g. ACTA) or cybersecurity (e.g. the Budapest Cybercrime Convention). But a combination of inter-state rivalries and political resistance from civil society have impeded their success. Russia and China, for example, have refused to sign up to the Cybercrime Convention, whilst proposing information security treaties of their own that define content regulation (i.e. censorship) as a matter

of cybersecurity. And ACTA was torpedoed by a transnational civil society movement. In the field of surveillance, countries suffer from information asymmetries or are confronted with practices against their citizens that might not comply with national or international standards. The recent ITU-conference in Dubai revealed various attempts to keep the governance of the Internet within a national context and outside international frameworks. There are interesting similarities between this debate and the governance discussions on broadcasting satellites in the 1970s and 80s (such as the 'receiving state' principle) (Queeney, 1978; The MacBride Commission, 1980).

Developing peer production and collective action mechanisms

One of the most contested areas of research is that of Internet-based political action. A lot of attention has been paid to the mobilizing effects of Internet use. The idea is that Internet-technologies radically lower the transaction costs of political activities and social action. This means they could potentially mobilize citizens and increased their political involvement. The empirical results, so far, are mixed. Most studies find a positive relationship between online activities and political action and interest. Some of these studies argue, however, that the citizens who engage in online activities such as reading news sites were already more interested in politics to begin with. Those who weren't already engaged, are left behind (e.g. Boulianne, 2011; Hindman, 2009). This is called the reinforcement effect. Other researchers found evidence that specific online political activities, whether passive (following the Twitter feed of a political party) or active (engaging in online forums), do increase offline political activities and social capital and mobilize people who were not yet politically active (Kruikemeier et al, 2013).

The potential for collective action also fuelled the hope that new forms of co-production between the state and its citizens would arise. These early hopes were driven by the highly visible successes of Wikipedia and open source software development (Benkler, 2006; Shirky, 2008). In practice, these hopes have met with mostly disappointing results. Many governments experimented with processes of peer production in their policy and political processes. But most wikis and other attempts to involve voters did not attract much participation. The early attempts were not really forms of peer production; the institutions' desire to prevent politically awkward situations and to secure 'high- quality' input meant they built curated environments which left very little room for organic political activity.

The emergence of social networks has created new forms of citizen input. Recent experiences suggest that these seem to be more effective in terms

of raising citizens' involvement. We should note, however, that this model moves away from the original idea of co-creation or peer production. Take the example of the 'crowd-sourced' new constitution of Iceland. Thousands of citizens commented on the text, partially via social media, but the articles were written by a Constitutional Council of 25 citizens who took the feedback into account. The final text was then approved by a referendum in which around half of the electorate voted. Elsewhere we also see how social networks enable feedback and to some extent dialogue between governments and citizens.

At the heart of these changes is the radical lowering of transaction costs. A Twitter message to a government account takes less effort than sending a formal letter and the same goes, to some extent, for the government's response. More importantly, that message and the response to it are at one and the same time one-on-one and broadcast to everyone else who cares to listen. One of the interesting characteristics of corporate Twitter accounts is that the 'voice' of the firm sounds a lot more like a human being than their other forms of communication. Probably because there is more direct contact with a human person. That in itself is no different from, say, call centres. The remarkable thing is not that there is a human responding, but that large corporate entities have empowered their 'webcare' teams to engage customers in a natural and seemingly free way – and that is quite different from call centres. For governments, this may be harder to achieve. Twitter messages can have legal implications, too. Such implications may constrain some uses of new media, making them more like the canned and carefully controlled communication channels of the mass media.

Lower transaction costs mean individuals can more effectively achieve some form of collective action. Many examples make clear that this also holds for politically-oriented collective action. Population ecology studies show that the nature of collective action changed dramatically as long ago the 1960s and 1970s with the rise of citizen activist groups (Mueller, Page and Kuerbis, 2004). The merits of new forms of collective action enabled by digital technology are hotly debated. Some observers dismiss them as 'slacktivism', where the action is little more than the feel-good measure of retweeting a tweet or liking a Facebook message (Morozov, 2011). The idea that the popular uprisings of the Arab Spring were somehow possible

because of the tools of Twitter of Facebook has drawn sharp criticism. Truly disruptive political activism is the product of strong ties between people who put themselves in harm's way, not of the weak ties between people who all contribute a little, so the critique argues. Current research does however show that social media produce new capabilities and a new style of activism, but that they are better at 'No' (stopping things or resisting abuses) than at 'Go' (building and exercising new governance capabilities) (Tufekci, 2013).

To some extent, this debate focuses on a misleading dichotomy. In reality, the online and offline forms of collective organizing can greatly enhance each other. Online tools have a mobilizing effect that reaches other segments of the population (Enjolras et al, 2012). The Obama presidential campaigns have also illustrated this. The online tools they used not only managed to mobilize an unprecedented number of people who donated multiple times to the campaigns, the online engagement was also a gateway to offline volunteering such as making phone calls, knocking on doors and attending rallies. Interestingly enough, because of the huge number of people involved, the campaign staff was forced to trust the local groups, which operated without staff supervision on behalf of the campaign. A certain degree of autonomy seems to be required for collective action to emerge. This is hardly unique to online environments, but it does suggest that there will always be a degree of tension between governmental attempts to seek peer production with their citizens and the kind of control that large public institutions, with their myriad accountability relationships, tend to seek. In that sense it is telling that the innovative use of online technologies in the Obama campaigns did not carry over into the Obama administrations.

We should also briefly note the persistent stream of literature that seeks to transfer the lessons of Internet businesses to the organization of governments. Typically, it translates the latest Silicon Valley success stories into a model for government (2.0, 3.0, etc.) and an answer to society's challenges. Technology can flatten hierarchies, data empowers people, government should be like a platform where citizens can build their own apps and come up with their own solutions, et cetera. This literature consists of business books rather than academic research, which allows its optimistic claims to

go largely unchecked by our existing knowledge about how complex public institutions work. In contrast, academic research has found that few of the supposed lessons are as straightforward as they sound. To illustrate: peer production is often less egalitarian than is frequently assumed and can be dominated by charismatic individuals or 'benevolent dictators', such as Linus Torvalds in the open source community around the Linux operating system (Kreiss et al, 2011). Many forms of peer production are implicitly dependent on – and in effect subsidized by – public and hierarchical institutions. For example, the largest group of contributors to Wikipedia are actually full-time or part-time college students and over 90% of the site's administrators have completed university courses or hold a master's or doctorate degree (Baytiyeh and Pfaffman, 2009). All in all, this implies that new forms of Internet-based collaboration complement the current mechanisms of collective action and joint production rather than rendering them obsolete.

Adapting to hyper-transparency

We used to speak of the Internet as an anonymous place. But as the ecosystem has become more developed, we have learned that Internet applications make social and technical processes hyper-transparent (Albrechtslund,2008; Andrejevic, 2005). Every single activity – logging on to a service at a specific time and date, one's geographic location and movement from one location to another, a purchase transaction, 'liking' something, sending a message, transferring a file – leaves tracks that can be digitally recorded, processed, stored and searched (Kuehn & Mueller 2012). Human activities, in all their glory, gore and squalor, take place in open, publicly visible mass-interaction platforms provided by commercial third parties. Even when they take place in more private, secluded online environments, these platforms generate storable, searchable records and their users leave attributable, recordable tracks everywhere (Brin, 1999).

The objectification of social interaction in the cyber-environment, and the ease with which we can rummage through the objectified remains, makes it a magnet for social control efforts (Lyon, 2007). The technological capacity to access these records and collect the data has vastly outstripped legal protections, leading to a rejuvenated privacy movement (Bennett, 2008). The fight for privacy frequently runs into paradoxes, because one of the main threats to privacy is users themselves. Research has consistently confirmed that offering users more comprehensive privacy controls over the data they share actually entices them to share even more online than without such controls. This is called the 'control paradox' – i.e. more control leads to more disclosure of personal data (Brandimarte et al, 2010). In this light, the successful campaign by activists to force Facebook to introduce better privacy controls might actually end up encouraging more sharing and publication of private information.

At the same time, hyper-transparency can support more bottom-up efforts to make government and businesses accountable. A number of open Internet bandwidth testing applications, for example, allow consumers of broadband services to determine whether their ISP is manipulating their

traffic in violation of network neutrality norms. Netizens in China have used 'human flesh search engines' to compile information about officials to expose and mobilize people around corruption and malfeasance, such as the railway official who was caught smiling insouciantly at the scene of a terrible train crash, and whose picture was rapidly disseminated to tens of millions via micro-blogs.

Our improved ability to see social activity objectified and recorded online leads to the (often incorrect) conclusion that the Internet itself is responsible for certain problems and that the problems visible there are rapidly growing. Politically ambitious prosecutors, from the U.S. to the UK to Italy, eagerly exploit such perceptions to propose or impose legal and regulatory constraints on Internet intermediaries. This process is robustly autonomous, and occurs even when the narrative is unsupported by – or is directly contradicted by – statistical data. It often lends itself to a displacement of social control efforts by inadvertently supporting the idea that human activity itself can be engineered and controlled by meddling with communication processes. When we see problems displayed in the online environment, or online tools are used to facilitate real-world crimes, we tend to link the two. Instead of controlling the behaviour, we strive to control the intermediary that was used by the bad actor. Instead of eliminating the crime, we seek to eliminate Internet access to the crime. It is as if we assume that life is a screen and if we remove unwanted things from our screens by controlling internet intermediaries, we have made life better and solved life's problems.

Hyper-transparency introduces new dimensions to the traditional societal practices related to cultural preservation and forgetting. On the one hand the digital environment creates huge challenges for those who would preserve information in an accessible and organized form. The simplest aspect of this problem is the torrential volume of new data created and the speed with which it changes. One digital preservationist site claims that due to inadequate preservation and archiving of the Web we are losing the equivalent of thousands of libraries of Alexandria every day. A more subtle and in some ways less tractable aspect of the problem is the rapid change in the physical and software form that information in the ecosystem takes. In the past, a writer using a typewriter to produce their manuscript faced

the problem of making sure the paper did not crumble into pieces or was not destroyed by water or fire. A contemporary writer may find that the novel or dissertation they wrote 30 years ago is not degraded physically, but is completely inaccessible because the writer used a discontinued form of word processing software and stored it on a Zip Drive, and neither the software nor the storage drive can be run on contemporary computers. A bewildering variety of standards gain ascendance and then become obsolete. Software programs for word processing, browsers, graphic display, file formats quickly come and go; so do different metadata standards and storage media.

To meet this challenge, an entire 'Digital Preservation' movement has grown up (McGovern, 2012). Some approaches are founded on the model of a traditional library-type 'repository', but that concept is not always suited to the dynamically changing form of Internet content. As an example of a new challenge, the U.S. Library of Congress has transferred and preserved Twitter messages from 2006-2010 and claims to be establishing a "secure, sustainable process for receiving and preserving a daily, ongoing stream of tweets." As of October 2012, the Library of Congress was receiving half a billion tweets each day, but must next confront the challenge of preserving the data in a way that provides usable researcher access to the archive. While this sounds fantastic to historians and social science researchers, it also means that years or even decades later we would be able to track the tweets of any individual as evidence of their state of mind.

As a direct countervailing trend to the goals of the digital preservationists, demands for a 'right to be forgotten' (RTBF) have been aired in some quarters (Mayer-Schönberger, 2010). Advocates of this right are concerned with the way the digital environment is becoming a one-way street where everything we do is recorded and stored and nothing is lost. This is alleged to imprison people in their past by making it impossible for them to change by escaping from or leaving behind prior statements, actions, inaccurate reports, and so on. Demands for a RTBF became popular with privacy advocates; the European Commission even made an effort to translate such a right into its data protection law (but seems to understand the complexity of it and has largely abandoned the original plans).

In theory, the RTBF would mean people could have their personal information removed from primary websites and any other sites that link to or republish the information. The right could apply in cases where, for example, information is being held for longer than needed by a business or where a person withdraws their consent to its continued publication. But the promise that the press of a button will apply a digital eraser to our recorded past is proving to be difficult to operationalize. Compliance with the right would be difficult and costly for Internet users, especially if it entailed tracking down third parties who had duplicated the user's information. Freedom of expression advocates tend to be hostile to the RTBF, fearing that it could be used to suppress political and public commentary. If RTBF is to be seriously considered, important exceptions to the right would have to be implemented, including for public health reasons, for historical, statistical and scientific research purposes, and for legal reasons regarding the commission of crimes. What remains after these exemptions is anyone's guess. As one journalist wrote, "rather than a right to be forgotten, we may end up with nothing more than a right to be frustrated."

Establishing identification and attribution

The emergence of hyper-transparency also impacts on the thorny and controversial issues of identification (Who is on the network?) and attribution (Who has initiated certain activities?). The Internet protocols themselves never contained user identification or attribution as part of their design (Cameron, 2006). These missing features have turned out to be both a blessing and a curse. While government policy options for increasing identification and attribution are being discussed at length, the market developments around hyper-transparency are already shaping the immediate future of identification, and might render the public policy debate more or less obsolete.

The core technologies of the Internet send, route and receive traffic between machines which are identified by IPv4 addresses and other technical identifiers. These identifiers are allocated in ways that make it very difficult to reliably connect them to specific persons or legal entities. To complicate matters further, there are ways to subvert the protocols. For example, it is technically very simple to spoof the originating IP address of traffic or the MAC address of a machine connecting to the network. These techniques are commonly used in certain forms of cybercrime, to make attribution difficult and identification even harder.

Only by adopting certain applications, technologies and procedures on top of the Internet as such can identification be ensured more reliably. For example, the corporate networks of firms can implement strict policies that only allow smart-card identified users with access to certain databases or services. Such technologies are only adopted in specific segments and niches of the Internet.

For most of the Internet, the connection between machines and persons or legal entities is loose at best. Take the WHOIS databases: the public record of who has registered a domain name or administers a certain part of the

IPv4 address space. WHOIS data is notoriously incomplete, outdated or just plain false. Law enforcement agencies have been lobbying organizations like ICANN for many years, asking for more stringent policies that increase the accuracy of WHOIS data, as well as making them more accessible for enforcement purposes. Privacy advocates have resisted these demands, noting that such registration records can be accessed by anyone, for any purpose, and thus violate standard data protection precepts.

So far, no real changes have been adopted, except in specific areas. China, for example, now requires citizens to provide their passport for identification before they can register a domain name under the Chinese country code top level domain. China is also the country which has implemented a technical protocol (Source Address Validation Architecture) that makes attribution of online activities to devices much more reliable and gives the government more control over which devices are on the network. Korea passed a law requiring the use of real names in certain instances, such as commenting on news websites, but abandoned it after huge numbers of national identification numbers were captured by hackers. Perhaps unsurprisingly, research suggests that forcing users to use real names on the Internet has a direct impact. It moderates bad behaviour such as using abusive language, but also seems to discourage certain positive behaviours such as providing valued counter-opinions. In this context, reference is often made to a right to anonymity. In legal theory, the right to anonymity is not considered to be an absolute right, but is often put into a functional context – for example, where it supports freedom of expression or is linked to the freedom of assembly.

In the absence of Internet-wide solutions, anyone who offers services on the Internet that require some means of identification has had to develop their own solution or use the identification solution of another provider. These solutions range from the use of cookies to arbitrary usernames to real name usernames to credit cards to government-issued and verified e-identities. Law enforcement organizations that have had to prove who was behind certain online activities typically assemble this proof from a variety of sources that help to tie an activity to a particular machine or person. Sometimes this is relatively straightforward, often it is cumbersome and sometimes it is virtually impossible (Clarke, 1994; 2008).

At policy level, there are competing forces at work for and against identity disclosure, even within the same country. Many countries provide privacy protections that shield Internet users from being identified against their will by other parties – 'Big Brother and little sisters', in the words of Castells – with whom they engage online. At the same time, governments have passed data retention laws that enable law enforcement agencies to track the online activities of citizens, and courts have required ISPs and other providers to hand over user data to other parties in civil or criminal litigation. An ironic illustration of these developments is the incident concerning David Petraeus, former director of the CIA. When one of his personal email addresses showed up in a routine inquiry, this triggered the question of whether someone else was posing as him. The subsequent investigation not only identified the director himself, but also the fact that he was having an extramarital affair, which was judged to be a security risk. He was forced to resign.

While the public policy debate on identification is still ongoing, developments in the market threaten to render that debate obsolete. Online providers have developed powerful ways to identify specific users. Google, for example, no longer simply relies on a username and password for identification: these can be too readily phished and abused, for example by criminals. Instead, Google looks at a variety of other signals during login, such as the IP-address being used and other technical cues that is has learned to associate with certain users. This helps to prevent accounts from being taken over by criminals who have obtained the user's password. Of course, the fact that Google knows how to collect and interpret these signals also means that Google can reliably identify the actual person across a whole range of activities. States are increasingly relying on these private identity technologies in law enforcement and intelligences activities. The irony is that the lack of public identity policies now enables states to piggy-back onto highly effective and intrusive private solutions. The recent revelations by Edward Snowden about the NSA's cyber-programmes have shown just how vast and comprehensive this identification and surveillance apparatus has become. It is a hybrid of private services supplemented with largely secret public surveillance technologies.

Such capabilities are not restricted to the Internet giants. Any site can purchase services for effective identification mechanisms, for example based on

device fingerprinting (Nikiforakis et al, 2013). Any device that connects to a site reveals all kinds of technical details about the software installed on the device, meant to help the site deliver the content in the most effective way. These configurations provide a unique fingerprint which is available to all sites that the user visits, irrespective of the user's use of cookies and other tracking technologies.[3] The implication seems clear: it is becoming more and more difficult to resist identification. For capable criminals, dissidents or privacy activists, it is worth the effort. For most of us, it has become practically impossible.

While traditional identification systems are being abandoned, the exclusivity of certain systems is also being explored. The Dutch government primarily relies on DigiD for its digital communication with citizens. In other countries, certain layers of the public administration allow third-party systems as an alternative (e.g. in Denmark, where Facebook identification can be used) or governments are experimenting with it. This development does impact on the role of the state as a trustee in its relationship with its citizens. In a sense, control is being transferred to these third parties, which are effectively taking over the trustee relationship. The European proposal for a new regulation on digital signatures may have as a consequence that third-party identification systems used by governments must be recognized in other jurisdictions. Several Member States have indicated that they would not support such a development.

3 See: https://panopticlick.eff.org/

Securitization and militarization

As society becomes more dependent on the Internet and digital services and devices, the vulnerabilities created by the interaction of software applications, devices and Internet protocols creates more opportunities for crime, vandalism, espionage, sabotage and information theft (Van Eeten et al, 2008, 2010). There are fears that the Internet could be used for terrorism by attacking what is regarded as critical infrastructure such as electrical power or financial systems (Dunn-Cavelty, 2008). Perhaps inevitably, these problems are being pressed into the framework of weapons and nation-state rivalries; cyberspace is now seen as a military 'domain' comparable to air, land and sea (Rosenzweig 2013). The U.S. military has created a cyber-command to develop and coordinate offensive capabilities (note that the term 'cyber warfare' seems to be used more often than 'cyber defence'). Other countries, including the Netherlands, are following suit. The logic of 'securitization' has been extended to the internet, as a new version of the military-industrial-university complex sucks more funding into this area and law enforcement organizations seek to extend their legal powers, as in the proposed Dutch law to allow the use of 'policeware' and the takeover of computers in other countries.

One significant aspect of this development is a digital arms race, as manifested among other things in a thriving market for 'zero-day exploits'. Zero-days are vulnerabilities that are not yet known to the producers and users of software. National intelligence and military agencies are using tax revenues to bid up the price for code and knowledge of problems. These vulnerabilities used to be exposed for smaller prizes and reputational effects, but their value to military and intelligence actors, who might use them to break into enemy systems, has greatly exceeded the gains that can be made by working in a more normal commercial/civilian context.

Is the cyber arms race of any real value? Often lost in the noise is the fact that real events have yet to confirm claims that cyber weapons are a revolutionary transformation of military capability. Despite constant warnings about a 'cyber Pearl Harbor', no actual uses of cyber weapons have ever

altered geopolitical relations, overthrown a state or displayed the level of destruction that the deployment of nuclear weapons did (Rid, 2012). The most powerful cyber weapon used so far – known as the Stuxnet attack – was compared by Michael Hayden, the retired former NSA and CIA director, to the August 1945 use of nuclear weapons against Japan, but in reality there is no comparison. Stuxnet delayed the Iranian nuclear programme for several months, but neither altered the Iranian government's determination to continue the programme nor undermined or overthrew the Iranian state itself. While Stuxnet was an incredibly sophisticated piece of computer programming which employed multiple exploits, its strategic effects were modest, to put it mildly.

Nevertheless, the growing sense that cyberspace is a military domain could project all the pathologies of nation-state competition (arms races, collateral damage, cold wars, alliances and technical incompatibility) into that domain. However, it should be noted that cyber warfare/defence has to meet the same democratic standards as 'ordinary' warfare, including sufficient legitimization and oversight (AIV/CAVV, 2011). It is not uncommon for the introduction of new technologies in warfare to challenge these standards, as the recent debates about the deployment of drones illustrate.

In sum

We have presented a concise overview of eight developments which shape the impact of the Internet ecosystem on the state and society at large. It bears repeating that such a survey can never claim to be complete. That said, these developments cannot be ignored. They are at the very heart of the challenges posed to the state by the increasing presence of Internet-based technologies in our society.

References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. Proceedings from Privacy Enhancing Technologies Workshop, Cambridge, UK.

AIV/CAVV (Adviesraad Internationale Vraagstukken/Commissie Van Advies Inzake Volkenrechtelijke Vraagstukken). (2011). *Digitale oorlogsvoering*. No 77, AIV/No 22, CAVV December 2011. Retrieved from http://www.aiv-advies.nl/ContentSuite/upload/aiv/doc/webversie__AIV__77__CAVV__22__NL(1).pdf

Albrechtslund, A. (2008). Online social networking as participatory surveillance. First Monday, 13(3). Retrieved from http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/ article/view/2142/1949

Anderson, S. P. & Gabszewicz, J. J. (2006). The Media and Advertising: A Tale of Two-Sided Markets. In: V.A. Ginsburgh & D. Throsby (ed.), Handbook of the Economics of Art and Culture, Elsevier, chapter 18, pages 567-614.

Andrejevic, M. (2005). The work of watching one another: Lateral surveillance, risk, and governance. Surveillance & Society, 2(4), 479-497. Retrieved from http://www.surveillance- and-society.org/articles2(4)/lateral.pdf

Baytiyeh, H., Pfaffman, J. (2009). Why be a Wikipedian? Proceedings of the 9th International Conference on Computer Supported Collaborative Learning 1. New York: ACM, 434–43.

Benkler, J. (2006). The Wealth of Networks: How Social Production Transforms Markets and Freedom. New Haven: Yale University Press.

Bennet, C.J. (2008). The Privacy Advocates: Resisting the spread of surveillance. Cambridge, Mass: MIT Press.

Boulianne, S. (2011). Stimulating or reinforcing political interest: using panel data to examine reciprocal effects between news media and political interest. *Political Communication* 28(2): 147–162.

Brandimarte L., Acquisti, A., Loewenstein, G. (2010). Misplaced Confidences: Privacy and the Control Paradox. Social Psychological and Personality Science, published online 9 August 2012. Retrieved from http://spp.sagepub.com/content/early/2012/08/08/1948550612455931.abstract

Brin, D. (1999). The Transparent Society: Will technology force us to choose between privacy and freedom? New York: Basic Books.
Cameron, K. (2006). The Laws of Identity. Kim Cameron's Identity Weblog. (January 8) http://www.identityblog.com/?p=354
Clark, R. (1994). Human Identification in Information Systems: Management Challenges and Public Policy Issues. Information Technology & People 7,4 (December) 6-37.
Clark, R. (2008). Dissidentity: The Political Dimension of Identity and Privacy. Identity in the Information Society 1, 1 (December) 221-228, at DOI 10.1007/s12394-009-0013-7
Dunn-Cavelty, M. (2008). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. London: Routledge.
Enjolras, B., Steen-Johnsen, K., Wollebæk, D. (2012). Social media and mobilization to offline demonstrations: Transcending participatory divides? New Media & Society, published online 26 November 2012.
Grant, J. (2011.) The National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy through Standards. Internet Computing, IEEE 15, 6 (November-December), 80-84.
Hall, R.B. and Biersteker, T. (2003). The Emergence of Private Authority in Global Governance. Cambridge: Cambridge University Press.
Hawkins, D.G., Lake, D.A., Nielsen, D.L., & Tierney, M.J. (Eds.). (2006). Delegation and Agency in International Organizations. Cambridge: Cambridge University Press.
Hill, K. (2012). Facebook's Top Cop: Joe Sullivan, *Forbes Magazine*, March 12, 2012. Retrieved from http://www.forbes.com/sites/kashmirhill/2012/02/22/facebooks-top-cop-joe-sullivan/
Hindman, M. (2009). *The Myth of Digital Democracy*. Princeton, NJ: Princeton University Press.
Introna, L., & Nissenbaum, H. (2000). Shaping the Web: Why the politics of search engines matters. The Information Society 16(3):1–17.
Queeney, K.M. (1978). Direct Broadcast Satellites and the United Nations, Sijthoff & Noordhoff.
Kreiss, D., Finn, M., Turner, F. (2012). The limits of peer production: Some reminders from Max Weber for the network society. New Media & Society, 13(2) 243–259.

Kruikemeier, S., van Noort, G., Vliegenthart, R., de Vreese, C.H. (2013). Unraveling the effects of active and passive forms of political Internet use: Does it affect citizens' political involvement? *New Media & Society*, first published online on July 11, 2013.

Kuehn, A. & M. Milton (2012). Profiling the Profilers: Deep Packet Inspection and Behavioral Advertising in Europe and the United States. Available at http://dx.doi.org/10.2139/ssrn.2014181

Latzer, M., Monroe E. Price, Saurwein, F. &/ Verhulst, S.G. (2007). 'Comparative Analysis of International Co- and Self-Regulation in Communications Markets', Research report commissioned by Ofcom - UK Office of Communications. Vienna: ITA.

Lenhart, A. (2009). Adults and social network websites. Retrieved from http://www.pewinternet.org/Reports/2009/Adults-and-Social-Network-Websites.aspx

Lyon, D. (2007). Surveillance Studies: An Overview. Cambridge: Polity.

MacKinnon, R. (2012). Consent of the Networked: The Worldwide Struggle For Internet Freedom. New York: Basic Books.

Mayer-Schönberger, V. (2010). Delete: The Virtue of Forgetting in the Digital Age. Princeton: Princeton University Press.

McGovern, N. (ed.) 2012). Aligning National Approaches to Digital Preservation. Atlanta: Educopia Institute. http://digital.library.unt.edu/ark:/67531/metadc98130/m1/1/

Morozov, E., (2011). The Net Delusion: The Dark Side of Internet Freedom. New York: PublicAffairs.

Morozov, E., (2013). Twitter message on 14 Jun 13, 1:25 AM, https://twitter.com/evgenymorozov/statuses/345320970472538113

Mueller, M.L. (2002). Ruling the Root: Internet governance and the taming of cyberspace. Cambridge, Mass: MIT Press.

Mueller, M.L. (2010). Networks and States: The global politics of Internet governance. Cambridge, Mass: MIT Press.

Mueller, M., Page, C. & Kuerbis, B. (2004). Civil Society and the Shaping of Communication-Information Policy: Four Decades of Advocacy. The Information Society, 20, 3, 169-185.

Nikiforakis, N., Kapravelosy, A., Joosen, W., Kruegely, C., Piessens, F., Vigna, G. (2013). Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting. Retrieved from http://seclab.cs.ucsb.edu/media/uploads/papers/sp2013_cookieless.pdf.

OECD (2010). The Economic and Social Role of Internet Intermediaries. Paris: OECD Directorate for Science, Technology and Industry. (April). Retrieved from http://www.oecd.org/sti/ieconomy/44949023.pdf

Pew Center. "New Media, Old Media." (2012). Pew Research Center's Project for Excellence in Journalism. 23 May 2010. Web. 28 June. <http://www.journalism.org/analysis_report/new_media_old_media>

Poort, P. & Leenheer, L. (2012). File sharing 2©12: Downloading from illegal sources in the Netherlands. Retrieved from http://www.ivir.nl/publications/poort/Filesharing_2012.pdf

RAND Media Group (2013). New Media vs. Old Media. RAND Media Group blog. http://www.randmediagroup.com/new-media-vs-old-media

Rid, T. (2012). Cyber War will not take place. The Journal of Strategic Studies 35, 1, 5–32. (February).

Rosenzweig, P. (2013). Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World. Santa Barbara: ABC-CLIO.

Shirky, C. (2008). Here Comes Everybody: The power of organizing without organizations. New York: Penguin Press.

Stol, W.P., H. K. Kaspersen, J. Kerstens, E.R. Leukfeldt, and A.R. Lodder. (2009). Governmental filtering of websites: The Dutch case. The Computer Law and Security Report. 25, 3, 251–262.

The MacBride Commission. (1980). Many Voices, One World, Rowman & Littlefield.

Thierer, A. (2012). The Perils of Classifying Social Media Platforms as Public Utilities. Working Paper 12-11 (March), Mercatus Center, George Mason University. http://www.scribd.com/doc/85833923/Social-Networks-as-Public-Utilities-Adam-Thierer

Tufekci, Z. (2013). Is there a Social-Media Fueled Protest Style? An Analysis From #jan25 to #geziparki Technosociology blog (June 1) http://technosociology.org/?p=1255

Van Eeten, M. and J. M. Bauer (2008). Economics of Malware: Security Decisions, Incentives and Externalities, OECD STI Working Paper 2008/1. OECD. Retrieved from http://www.oecd.org/dataoecd/53/17/40722462.pdf

Van Eeten, M., J. Bauer, H. Asghari and S. Tabatabaie (2010). The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data. STI Working Paper 2010/5. OECD. Retrieved from http://www.oecd.org/officialdocuments/displaydocument/?doclanguage=en&cote=dsti/doc(2010)5

Van Eijk, N.A.N. M., T.M. van Engers, C. Wiersma, C.A. Jasserand and W. Abel (2010). Moving Towards Balance: A study into duties of care on the Internet, WODC/University of Amsterdam.

Van Hoboken, J., A. Arnbak, N. Van Eijk (2013). Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act, SSRN. http://ssrn.com/abstract=2181534

Wagner, B. (2013). "Governing Internet Expression: How public and private regulation shape expression governance." *Journal of Information Technology & Politics* 10, 3.

Whinston, A.B., Stahl, D.O., & Choi, S.Y. (1997). The Economics of Electronic Commerce. New York, NY: Macmillan.

WRR (1998). Staat zonder land: een verkenning van bestuurlijke gevolgen van informatie- en communicatietechnologie, WRR rapport nr. 54.

Zhang, K., & Sarvary, M. (2011). Social media competition: Differentiation with user-generated content. Working Paper, INSEAD. http://www.stern.nyu.edu/cons/groups/content/documents/webasset/con_032240.pdf