Surveillance & Society

Article

Networks and Resistance: Investigating online advocacy networks as a modality for resisting state surveillance

Lucas D. Introna

Lancaster University, UK. mailto:l.introna@lancaster.ac.uk

Amy Gibbons

Lancaster University, UK. mailto:a.gibbons1@lancaster.ac.uk

Abstract

This paper explores the network of relationships that emerge from the online activities of privacy advocates. It argues that this advocacy network, through its linking practices, may potentially become a network of meta-surveillance that has the potential to transcend the agency of the individual actors. By reducing the degrees of separation between the actors, through their linking practices, the network can foster links between different sets of data, create links between information about incidents, corroborate information (making it more credible), direct the attention of the public and the traditional media to particular state surveillance practices, and so forth. Through these linking practices the network can draw upon the emergent positive network externalities to realise an information politics that is beyond what any single actor can achieve. Through the use of social network analysis and a webometrics methodology (supported by web-based crawling applications) we attempt to reveal this emerging online advocacy network. Through our data collection and analysis we show that the online advocacy network seems somewhat fragmented with a relatively small but stable, and geographically biased, core. This tentative analysis and conclusion may have important implications for the way privacy advocates view their online practices.

Introduction

> ‘Pressure groups and advocacy organizations working on the margins of the actual legal processes usually play a part in obtaining the eventual legislative change. But such groups also make a contribution to the ‘struggles over surveillance’ in their own right. Although they have not yet been studied systematically, it is worth examining the activities of such groups. While they may not count as a fully fledged ‘social movement’, they are undoubtedly influential in the field.’
>
> David Lyon (2007: 173)

The issue of data protection and privacy have been very prominent in the UK media of late due to a number of significant data handling breaches—with the subsequent loss of very large (and sensitive) data sets. These incidents have raised serious questions about the government’s ability to secure the personal information of its citizens. Given the often hidden nature of the use and storage of citizen data—once it has been relieved of its owner—the ways in which to monitor or indeed resist the data collection and

Introna, Lucas and Amy Gibbons. 2009. Networks and Resistance: Investigating online advocacy networks as a modality for resisting state surveillance. *Surveillance & Society*, 6(3): 233-258.
http://www.surveillance-and-society.org | ISSN: 1477-7487

handling practices of governments have remained elusive. Sousveillance—the view that we can invert the all seeing eye of the panopticon—may allow for the actions of the watchers to be exposed and may subsequently engender a certain level of accountability on the part of the state. But who will engage in such sousveillance on behalf of the citizen? One logical suggestion would be for this to be done by advocacy groups. But, as David Lyon (2007) highlighted, the study of advocacy groups, whose purpose one might say is to enlighten the public on issues of privacy and who may act as the watcher of the watchers, have hitherto received little systematic academic attention—the recent book by Colin Bennett (2008) being a notable exception.

Public collaborations between privacy interest groups, such as for example the Surveillance Studies Network's (SSN) joint paper with the UK Information Commissioner's Office on a Surveillance Society (2006), and other individual publications (Liberty, 2007; ACLU, 2003, 2007a, 2007b) at least in some way presupposes the notion of some broader advocacy movement, or network of action and resistance, to counter the perceived excesses of state surveillance (especially post 9/11). If there is indeed such a broader advocacy movement then one might argue that the possibilities for resistance, for the citizen, lies within the combined collective action (or the network of more or less coordinated action) of these actors and their intermediaries. In this paper we want to suggest that the collective agency (intended or unintended) of these combined advocacy actors—as an emergent online network—may have the propensity to exert pressure on the asymmetrical power imbued by the state,[1] through strategies such as 'information politics',[2] amongst others, and as such act as one possible mechanism for resisting state surveillance practices—possibly constituting what one might call a network of *'meta-surveillance'*[3] (i.e. for watching the watchers).

In order to develop this argument the paper is structured as follows. First, we explore the importance of networks, with a specific focus on the activities of advocacy groups on the Internet. We discuss how the linking patterns of these groups can potentially constitute a network with emergent positive network externalities that often transcend the intentions and possibilities of individual advocacy actors. Second, we discuss the need and mechanisms for resisting state surveillance. We argue that on the one hand we are seeing the rapid expansion of state surveillance of citizens' activities (often under the seemingly legitimate need of security or more efficient government) and on the other hand we see a rather rapidly declining trust, by the citizens, of the ability of governments to adequately secure the data collected. It is, however, not clear (or may not be possible) for individual citizens to resist state surveillance practices. Some have argued that it is the role of advocacy groups to step forward to expose and make visible these practices, so as to enact resistance and possible accountability (Bennett 2008). But how can advocacy groups do this? We suggest that they may do this by becoming an expanding and cohesive online network for information politics and meta-surveillance. In the third part of the paper we use social network analysis (SNA) to attempt to reveal and analyse the hyperlink structure of the online advocacy network. In doing this we explore the extent to which this advocacy network can be seen as a cohesive network that may have the potential to resist the practices of state surveillance. We conclude the paper with some preliminary findings from our analysis, as well as some suggestions for an ongoing research project.

[1] We use state as an umbrella term to encompass a range of governing bodies worldwide

[2] Information politics "relies on the ability to generate politically relevant information and move it by the most effective means to the place where it will have the most impact, at the most critical time" (Bennett 2008, 96).

[3] Although the term 'meta-surveillance is mostly used in the medical context for the monitoring of simultaneous disease outbreaks, we will use the term 'meta-surveillance' in this paper to imply bringing together of a variety of resources in order to generate the conditions that would allow for 'watching the watchers'.

On the virtue of virtual networks

The well known theory that every person in the world is interconnected by a mere six degrees of separation[4]—the so-called small world hypothesis—statistically requires that each individual will have at least 100 direct relational contacts, such as friends or family (Watts 2003). These relational contacts are likely to share mutual links, with other contacts, thereby introducing certain possible *clusterings* (or sub-networks) in the network. Urry (2007) argues that if one simply considers the family and friends network, this alone will provide a too large degree of socio-spatial separation for the six degree hypothesis to be feasible; what is needed is the intersection of other intermediary actors such as organisations and technology to link to a wider audience. For example, *Facebook*, the popular social networking site, can be seen as an example of such an intermediary.[5] Indeed, as is known, this media has transcended its virtual boundedness and started to connect to other avenues of life, including work, with some job sites[6] warning that the success of job applications can be as much based on information obtained through social networking sites, such as *MySpace*, *Bebo* and *Facebook*, as the information volunteered by the applicant on application. Although the small world hypothesis has been contested in a variety of contexts, it is nevertheless helpful in highlighting the importance of networks and the possibilities for networking that they may imply. But more than that, the ways in which networks, through network effects, transcend the intentions and agency (one might say reach) of individual actors within it. Of course, intuitively we know this and, as researchers, we also see this for example in the way citation analysis supposedly reveals influence and the impact of research beyond the intentions of individual researchers.

There has been some research to show that the small world hypothesis does apply to the hyperlink structure of the Internet under certain conditions (Adamic & Adar 2001; Broder *et al* 2000; Thelwall & Wilkinson 2003; Park & Thelwall 2003). What is disputed is the degree of separation that applies in this context. In some cases it has been shown to be approximately six (Adamic & Adar 2001) in other cases it might be as much a sixteen (Broder et al 2000). As one would expect it is significantly lower when one is located within a particular sub-network (such as Facebook for example) than it would be between any randomly selected web pages in the world-wide web as a whole. It is therefore feasible to suggest that any potential visitor with a particular search interest and an ‘appropriate starting point’ should be able to find what they are looking for through navigating more or less six hyperlinks. An ‘appropriate starting point’ is here taken to mean a starting point that locates the searcher in the relevant sub-network. How would searchers find ‘appropriate starting points?’ Normally, when searching for information on a particular topic area on the Internet, a visitor is likely to perform one of two tasks: 1) enter the name of a web address they know contains the type of information they are looking for or 2) more likely, type relevant keywords into a search engine and follow the most applicable link from the list provided. In the first instance the visitor knows the site which contains the type of information being sought; this obviously significantly reduces the number of links they need to use. In the second case the visitor will find the appropriate starting point by using the references (links) in a site of interest, or by using the list provided by the ranked recommendations of the search engine—which is also itself based on the linking patterns of sites. In other words the context sensitive linking patterns of sites, by their very nature, reduces the degrees of separation between relevant or related sites, *thereby constituting networks (or subnetworks) of common or shared interests*. It is important to note that these sub-networks emerge without the link creators necessarily wanting to constitute them as such—i.e. as an implicit outcome of normal linking behaviour and patterns of web content creators and editors. This is the benefit of context sensitive imbedded (hyper)linking, which is at the heart of the network organisation of the web—and the

[4] The ‘degrees of separation’ is the number of links one would need to transverse to get from any given node or actor in the network to any other given node or actor in the network.

[5] The six degrees of separation experiment is also active on Facebook through a series of applications and groups, one such example can be found here: http://www.facebook.com/apps/application.php?id=4616854023 (accessed November 2, 2008)

[6] An example of such a story can be found on the Equinox site: http://media.www.keeneequinox.com/media/storage/paper537/news/2008/10/30/Opinions/Employer.Surveillance.Of.Social.Network.Sites.Like.Facebook.And.Myspace.Bodes.Il-3511588.shtml (accessed November 3, 2008)

success of the Google search engine for that matter. However, not all of these sites (or *actors* as we shall refer to them) have equal status in the sub-network, some are at the core and some are in the periphery.

If we consider a particular hyperlink sub-network (or 'installed base' as referred to by Ciborra (2002)) in the global world-wide web network, then we are likely to encounter a relatively stable *core* of actors that are steadily affecting changes in the *periphery* through their ongoing linking practices. These *core* actors tend to have a high level of visibility (through advertisement, word of mouth or search engine prominence) and as such are disproportionately likely to be visited and linked to repeatedly, thus, affording them growing importance or *centrality* in the network. As Barabási explains:

> 'the bottom line is that when deciding where to link on the Web, we follow preferential attachment: When choosing between two pages, one with twice as many links as the other, about twice as many people link to the more connected page. While our individual choices are highly unpredictable, as a group we [tend to] follow strict patterns' (2002:85).

Once linked, the visitor's experience is then arguably constructed by the site as they attempt to guide their visitor down particular avenues of interest. The more time that is spent on the site, in principle at least, the more knowledge is gleaned for self-interest or dissemination purposes. There are, of course, external constraints on this process to be aware of, such as the following: technological know-how, economic factors (cost of staying on the Internet browsing), knowledge of the topic area being searched and recommendations from personal networks.

Barabási (2002) suggests that there are certain intrinsic power laws that operate in such sub-networks. One of the most central theories is that the power to successfully expand a network lies with the core actors. Sites on the *periphery*, i.e. the weakly linked to sites, might contain information which could be of benefit the whole network, but only if they are rendered visible to other actors in the network—i.e. are drawn into the network through increased linking (Buchanan 2002). One might argue that it is therefore in the interest of the core actors to continually search for and post up-to-date links to relevant sites on the *periphery*. As these sites are pulled closer to the centre of the network the sites they link to, which may previously have only existed outside this specialised network, on the wider world-wide web, will themselves be pulled in, creating a greater level of interconnectedness to the benefit of the whole network. Differently stated, it would increase the density of the network; and the higher the density of the network the lower the degrees of separation between any two actors in the sub-network. Increasing the density of the network is often referred to as positive network externality, i.e. where benefit is unintentionally created for the whole network through the behaviour of mostly self-interested individual actors. Thus, such behaviour would create a virtuous cycle of interconnectedness (density or cohesion) and increased visibility *for all the members of the network*.

Drawing on these principles of networks, and the hyperlink structure of the web, we would argue that the individual *actors* that are concerned with state surveillance (such as privacy activists, advocates, researchers, etc) can potentially, through their linking practices, constitute a network that has, as one of its network externalities, the possibility of being a cohesive network of *information politics* and *meta-surveillance*. In other words through their linking behaviour (and the information they make available through such links) actors in the sub-network can develop a collective awareness of emerging state surveillance practices—by for example following up and linking together incidents, corroborating information, making links between different data sets, and so forth. But to what degree does such an online advocacy network exist and act in the ways suggested? One way to answer this question is to attempt to reveal this network through a network analysis of its hyperlinking structure, using relevant tools and techniques (Borgatti *et al*. 2002, Nooy *et al*. 2005). However, before doing this we want to suggest why some have argued that such a meta-surveillance network (as a mode of resistance) may be seen as increasingly necessary.

On the need and mechanisms to resist state surveillance

> ‘The State is superstructural in relation to a whole series of power networks that invest the body, sexuality, the family, kinship, knowledge, technology and so forth. True, these networks stand in a conditioning-conditioned relationship to a kind of ‘meta-power’ which is structured essentially round a certain number of prohibition functions; but this meta-power with its prohibitions can only take hold and secure its footing where it is rooted in a whole series of multiple and indefinite power relations that supply the necessary basis for the great negative forms of power.’ (Foucault as cited in Gordon 1980: 122)

The asymmetric power relationship that the state has over its citizens is problematic for those who want to enact resistance. Krotosynski (1990) claims that in free societies the government is selected by the people from a range of candidates and therefore the issue of privacy rights (or lack thereof), as enacted by government, could be seen as an indirect measure of society’s commitment to liberty and, in a broader sense, to autonomy. However, to really make this choice the citizen needs to have access to a high level of transparency of state action. Such transparency, although very desirable for the citizen, is not necessarily in the interest of governments since, as Lyon (2007) highlights, the more subtle the surveillance regime the more likely it is to have the desired effect. One could therefore argue that one important element of resistance—one which will enable real choices in the democratic process—lies in the ability of different actors to make visible the variety of state surveillance practices and the connections between such practices. Indeed, a lack of such accountability was one of several antecedent factors attributed to the UK’s rating an ‘endemic surveillance state’ (Privacy International 2006), especially in the areas of constitutional protection, identity cards, biometrics, data-sharing and, communications interception (2007).

Technology and information processing often act as an intersecting layer between the ‘body’ and the ‘state’, which can be witnessed in most public sector organisations, through for example ID cards, medical histories, driving licences, passports and more recently biometric scanning in schools (in the UK). Under state protection principles giving up one’s personal data is not only advised, it is indeed compulsory (Haggerty and Ericson 2006). Although several countries have legislation in place to prevent the sharing of data across internal state departments,[7] once the data has been collected there is no guarantee of its future use (Raab 2003). Furthermore, knowledge discovery technology in large databases (KDD) is a growing problem for normative privacy (Tavani 1999). We also know that the larger the data set the higher the probability of inaccurate or erroneous data. These databases often have unique identifiers, for example a National Insurance number or NHS number, that can be use to facilitate the process of performing relational queries with other databases, thereby establishing connections and the building up of what Roger Clark calls the ‘digital persona,’ with associated ‘dataveillance’ practices (Clark 1994). This is one of the reasons why the national ID card is facing such strong opposition in the UK. In the proposed system a National ID number would act as a master key to link and unlock all data across all government databases. Liberty’s research into ‘Surveillance and Personal Privacy in Modern Britain’ showed that the British people’s faith in government data handling practice is dwindling. In a *YouGov* Poll, commissioned by Liberty in 2007, ‘54 per cent of those questioned did not trust the government and other public sector authorities to keep their personal information completely confidential’. When it comes to state surveillance we seem to see two opposing trends. On the one hand we see the rapid expansion of state surveillance of citizens activities (often under the seemingly legitimate need of security or more efficient government) and on the other had we see the decline of citizens trust in the ability of governments to secure the data collected—especially if this data is in an electronic format.

[7] In America the Total Information Awareness (TIA) Project was disbanded in 2001 following civil liberties campaigns. However similar projects continue to be implemented elsewhere for example the Golden Shield Project in China where laws are less restrictive on the collation of personal data.

Nearly every major government department has experienced some form of public data loss in recent months; at the time of writing this paper the UK Home Office had just admitted to the loss of some 84,000 criminal records, stored on a memory stick by the firm PA Consulting, during a research project[8]. This is the latest in a series of public failures; in November 2007 two discs containing the records of every child benefit claimant were lost in the UK[9] and an employee of the US Department of Veteran Affairs' laptop was stolen, containing the records of 26.5 million veterans, including their social security numbers and, in some cases, disability ratings[10]. Research conducted by the *Telegraph*[11] reported 37 million items of personal data had been lost in 2007 by government officials. The ACLU report 'Bigger Monster, Weaker Chains' examined the American 'surveillance society', specifically the dangers of commercially collected data being obtained through government channels; "although the Privacy Act of 1974 banned the government from maintaining information on citizens who are not targets of investigations, the FBI can now evade that requirement by simply purchasing information that has been collected by the private sector." (ACLU 2003:8). Kerr (2007) argues that society is rapidly moving away from retributive justice, based on the redistribution of wealth and punishing wrongdoers, to actuarial justice where the state uses profiles, statistics and behavioural predictors to assess risk, generate suspicion and pre-empt threats to safety. These invisible processes of classification, codification and categorisation (Suchman 1994) into a 'digital persona'—which acts as a *true* yet digital representation of the actual self—"does not determine a person's actions; it [merely] provides the space of action which one can move" Winograd (1994).

In response to the legitimate concerns of citizens some institutional mechanisms have been created such as Information and Surveillance Commissioners. These bodies are supposed to create some symmetry of power between the state and the citizen. They are, however, often seen as too close to government to be an effective mechanism of resistance. Another, generally accepted, mechanism of resistance is the use of advocacy groups (Bennett 2008). Indeed historically advocacy and pressure groups have long proved useful in mediating civil issues with governments, for example the abolition of slavery and woman suffrage (Keck and Sikkink 1998). A European Commission (EC) paper on building stronger partnerships with non-governmental organisations (NGOs) argues for a stronger role for *advocacy NGOs* whose 'primary aim is to influence the policies of public authorities and public opinion in general' (European Commission 2000:4). It is this work of *privacy advocates* who perform the function of advocacy NGOs, within the domain of state surveillance, which is our concern here.

In his book "The Privacy Advocates" Colin Bennett (2008, 59) makes the case for an active and vibrant network of privacy advocates. He argues that although there is a network this network is "dynamic, volatile, overlapping, fragmented and somewhat elusive". He further suggests that there is "certainly no clear structure…neither is there a social movement with an identifiable base…perhaps [there is] an 'advocacy network,' which can be conceptualised not as a fixed structure, but as a series of concentric circles." It is this network, in as much as it can be said to exist, that our research wants to identify and attempt to reveal. It is our claim that such a virtual network may be a powerful actor through the enactment of *information politics*[12] in particular. The success of such as network's information politics—i.e. ability to generate politically relevant information and move it by the most effective means to the place where it will have the most impact, at the most critical time—will in part be facilitated by the cohesiveness and density of the network as well as how this network interconnects with other relevant

[8] See http://news.bbc.co.uk/1/hi/uk_politics/7575989.stm (accessed November 2, 2008)

[9] See http://www.guardian.co.uk/politics/2008/jun/26/whitehall.children (accessed November 2, 2008)

[10] See http://www.computerweekly.com/Articles/2007/11/20/228208/us-department-of-veteran-affairs-in-yet-another-data.htm (accessed November 2, 2008)

[11] See http://www.telegraph.co.uk/news/newstopics/politics/1574687/Government's-record-year-of-data-loss.html (accessed November 2, 2008)

[12] Bennett (2008, 96) suggests, with reference to the work of Keck and Sikkink (1998), that advocacy groups engage in a fourfold typology of tactics: information politics, symbolic politics, accountability politics and leverage politics. We would suggest that advocacy networks on the internet is particularly important for information politics (although it obviously does not exclude the other forms of tactics)

actors such as information and surveillance commissioners, traditional media, new media, researchers and so forth. It is our proposition that an effective enactment of information politics by the network will be an essential constitutive element of a meta-surveillance network, which in turn is an important element of resisting state surveillance practices. This will be the focus of our network analysis in the sections that follow.

On the constitution (or not) of an online advocacy network

This paper proposes to use the principles of social network analysis (and network principles more generally) to explore the manner in which it can be said that online advocates do constitute a more or less cohesive network (which may function as a viable mode for resisting state surveillance) and to show how this network relates to a wider network of intermediaries that they rely on to disseminate their information, i.e. to enact their information politics. In the subsections that follow we outline our methodology and the initial research conducted into the network of privacy advocates, which was done using publicly available web crawling applications (i.e. *SocSciBot*[13] and *IssueCrawler*[14]).

Social network and webometric analysis as a methodology

Social network analysis (SNA) has been used in various disciplines to analyse the interactions between different groups or sub-groups of society. For example it has been used to study communication networks in organisations, the diffusion of innovation, informal collaborations in research groups, and so forth (Freeman 2004). Through SNA it is possible to get a sense of certain group or network characteristics such as: the cohesiveness of a group, who the central actors are, who are on the periphery, and so forth. Traditionally SNA is done by collecting data through interviews with the relevant actors or by compiling data from public sources about relationships (such as equity ownership between different companies). Increasingly SNA methods are also being used to investigate the relationships between internet actors (websites, web pages, etc) using publically available hyperlink data. This is referred to as 'webometric' methods. Webometric based studies have focused on a variety of topics such as: the performance of search engines (e.g. Courtois and Berry 1999; Hawking et al 2001; Thelwall 2000; Thelwall 2002; Vaughan and Thelwall 2004); the mapping of (issue) networks (e.g. Garrido and Halavais 2003; Garton et al 1997; Rogers 2004; Rogers and Marres 2000; Van den Bos 2006; Wormell 2000), the mapping of blogs and social networking (Adamic and Glance 2005; Hargittai 2007; Lin and Halavais 2004; Thelwall 2007a; Thelwall 2007b; Thelwall and Hellsten 2006), and so forth.

All of these studies have one assumption in common. They all assume that hyperlinks are contextually meaningful or socially significant in some way or another i.e. that a link is not merely a pointer that simply happens to refer to a computer address (or IP address) somewhere in cyberspace. They all assume that there are, more or less, significant reasons why authors create links between themselves and other nodes (or *actors*) on the Web. Foot et al (2003) suggests that "actors on the web acknowledge other actors by linking to them" and as Rogers claims "non-linking is a form of non-recognition and is an act of silencing through [such] non-recognition" (as cited in Foot et al 2003). Thus, through the creation of links relevance, recognition and acknowledgment are often enacted. Obviously, not all links function in this way and some are indeed done for rather more trivial or instrumental reasons, such as trying to improve search engine ranking. However, when a large amount of links accumulate between actors it can no longer be dismissed as insignificant. Indeed linking patterns and link counts are the fundamental basis upon which the issue of relevance is decided by the Google search engine (Introna and Nissenbaum 2000). Given the success of the search engine, based on these link patterns, one can reasonably claim that context sensitive link patterns can legitimately form the basis for a SNA—i.e. they do in some way designate contextually meaningful relationships rather than random or trivial links. If this is the case then one must still answer the question about what can be known from such an network analysis of linking patterns and,

[13] http://socscibot.wlv.ac.uk (accessed November 1, 2008)

[14] *IssueCrawler.net.* http://www.govcom.org/Issuecrawler_instructions.htm (accessed March 10, 2000).

furthermore, how might one go about doing it. We will take up the first part of the question when we do the analysis below. In response to the second part of the question we will propose a methodology for doing the analysis which is partly based on the work of Hsu (2008).

As indicated above, the central question that informs this research *is whether online advocacy groups concerned with state surveillance can be said to constitute an emergent network of meta-surveillance, which can, through information politics, act as a possible mechanism for resisting state surveillance practices*. A first step to answering this question is to understand how, if at all, this online network is constituted. Who are the actors in this network, how dense is the network, how do they interconnect (who are central, who are on the periphery), and so forth. A subsequent step in the research would be to analyse traffic as well as more in-depth interviews with different actors in the advocacy network. One might also track and analyse how major incidents get absorbed and communicated through the network, and more. The initial research reported here aims, as a first step in this project, to reveal links between advocate groups including any 'intermediaries' they may use to relay their information and messages.

In trying to make this online network visible, or analysing any network for that matter, a key question is to establish a methodology to draw appropriate boundaries of the sub-network. At one end of the spectrum the whole internet is the network since every actor is connected to every other actor even if it is through massive degrees of separation. On the other end of the spectrum is a network that consists only of one actor and all those that are directly connected to it. Clearly these two extremes are not helpful ways of drawing appropriate boundaries. In order to solve this problem the research needs a more or less rigorous methodology to decide who is part of the network, who is not, and why? In other words such network research needs to have a methodology for drawing network boundaries in a meaningful and appropriate way. In traditional SNA one would ask the actors where the boundaries are. How would one do this in a webometrics analysis?

Establishing the network boundaries: the initial actor selection process

Eight, well-known, privacy and surveillance centric sites (the American Civil Liberties Union (ACLU); Consumers Against Supermarket Privacy Invasion And Numbering (CASPIAN), the Electronic Frontier Foundation (EFF), the Electronic Privacy Information Centre (EPIC); Liberty; Orwell Awards; Statewatch and the Surveillance Studies Network) were used as the initial pilot sites, or staring points, for the research using an actor-centric (also known as the ego-centric) approach. This entailed each actor being *crawled*, in turn, to determine the sites that they linked to, drawing comparators with other sites to reveal those core (densely linked to) sites in the network. These pilot crawls proved useful however there was a likelihood that they only represented a certain proportion of the network, which were based on popular privacy and surveillance reports and news items. We were also aware of other interesting forms of electronic advocacy that did not entail the publishing of reports as such.[15]

As mentioned, for the crawls we used *SocSciBot* and *IssueCrawler* and their affiliate programs *UCInet*[16] and *Pajek*[17]. *SocSciBot* (Social Science Bot) is a custom crawler developed by Mike Thelwall, of Wolverhampton University, which provides the user with a vast amount of detail of the individual structures of sites, including all page content. For the second, more exploratory task of revealing the network (the overall network and sub-networks) a crawler called *IssueCrawler*, devised by Richard Rogers and the *govcom.org* foundation, was used (to be discussed below). This tool provides the functionality of not only looking at the initial sites provided but also looking at the sites that they link to,

[15] An example of this is the Tracking Transience website. Developed by Hasan Elahi, an Assistant Professor and media artist, this is an example of an extreme act of sousveillance, by a man who was once mistakenly listed on a terrorist watch list. Since then he has turned his private life inside out by placing a Global Positioning System (GPS) tracking device in his mobile phone so that he is instantly locatable, via Google, 24/7 and as a means of verifying his existence, posts images to his website of his surroundings on a regular basis.

[16] http://www.analytic.com (accessed November 1, 2008)

[17] http://vlado.fmf.uni-lj.si/pub/networks/pajek/doc/pajekman.htm (accessed November 1, 2008)

and where they link to, ultimately creating a network based on cross-referencing and link density.[18] Therefore, if an important actor had been missed in the initial selection process (which was based on data collated from the pilot sites) then this crawler would extrapolate to those missing nodes and fill in the blanks, so to speak. A detailed flow diagram of the actor selection process can be found in *Appendix 1*. The govcom.org website, home of the *IssueCrawler*, provides recommendations for establishing the initial core set of actors to use to ascertain a particular 'issue network' as they call it:[19]

1. *Use a search engine such as Google and use the top ten or twenty results. Also use any contacts or 'experts' within the field, details from newspaper articles, a particular organization's website with recommended links and any other recommendations to gather an initial list of useful websites.* In this case a keyword search was conducted through Google resulting in approximately 295 actors.
2. *Avoid using big media sites and big portals as they have links to a wider range of sites, not all of which will be relevant and 'do not produce 'networks.'* We only included sites that had clear messages regarding *state surveillance*. There are examples of advocates that were not used, because their focus was on other human rights issues, for example Amnesty International.
3. *Find the relevant page on a website and use that as a starting point i.e. the ones that pertain specifically to the issue under investigation*: This step was changed slightly due to the vast network and sub-networks being dealt with (approximately 57,594 links for the external link count and a further 880 from the Google search, before filtering). We had to balance the aim of wanting all relevant sites and a need to focus on those that had the issue of state surveillance as a core focus.
4. *Deleting duplicates:* this was perhaps the most time consuming task. The 2,803 links (returned from Google and pilot tests[20]) were stripped back to their domain name for categorisation. Duplicates were deleted a total of three times over the course of the filtration process.

The basic principle of the approach used here is to allow the actors to indicate the relevant actors and boundaries of the network through their linking patterns. By using a system of ongoing cross-referencing the crawlers progressively include actors, for subsequent crawls, which have multiple links from already known actors. This iterative process is continued until no new actors emerge. The success of this methodology is obviously dependent of very carefully selected starting points (hence our careful selection of the initial starting points in this step).

Refining and revealing the advocacy network through sociograms

Using our key actors, established in the previous step, as starting points *IssueCrawler* was set up to run at frequent intervals. The research was conducted over a period of four months, a crawl being conducted every fortnight[21]. This was done for two reasons: first, we wanted to determine the stability of the network and, second, we wanted to see whether specific state surveillance incidents were reflected in the link activity of the network. The crawl itself is not aggressive i.e. it does not constitute an unnecessary workload on the servers of the sites being crawled (Thelwall and Stuart 2006) and we ensured the actors crawled were relevant, to reduce waste. This is an important consideration for this type of research.

In using *IssueCrawler* the proportion of new actors in the network, those not already established in the initial filtration process described above, was 46%[22]. This suggests that one can have reasonable

[18] This has predominantly been close to 100 links, usually averaging around 95 links which does pose the question for social network analysis more generally of if this is a common denominator when it comes to link count.

[19] These have been adapted from the original website - http://www.govcom.org/Issuecrawler_instructions.htm (accessed November 3, 2008)

[20] To try to ensure that only relevant sites were included in the 'harvest', only those 'actors' with a link count of two (2) or more were included in the process.

[21] The crawls were conducted fortnightly between the 2nd August and 8th November 2008. Further research is being undertaken at present to analyse this data temporally to ascertain any difference. The crawls are scheduled to continue fortnightly until 3rd January 2009 to allow 6 months data collation.

[22] This includes actors in the *core* and *periphery* of the network, as described later in the paper

confidence in using a combination of Google (a commercial search engine) and *SocSciBot* (a private crawler) in determining relevant network actors for a given criteria, as was done in the first step. As previously stated the *IssueCrawler* application works by 'harvesting' the sites given to it by the user, then analysing those links, as well as the links in those sites to other sites and so on, all the while cumulating the number of links till it comes full circle and determine the most prominent actors. In other words membership of the network—i.e. the boundaries—are determined by the context sensitive links or references provided by the actors themselves. Through this process of cross-referencing (and link density criteria) *IssueCrawler* provides its list of network members. We would suggest that the triangulation between Google, *SocSciBot* and *IssueCrawler* provides one with a fairly robust methodology, for actor selection in determining the boundaries of the network—given a certain link density threshold. At the end of this selection process the advocacy network comprised of 128 intermittent actors, 74 regular actors and 35 new actors (these are listed in *Appendix 2*). So far in our *IssueCrawler* crawls completed 26% of the originally selected actors have appeared in the network as reflected in the network diagrams below (19 on the first crawl on 2nd August and 2 more on 30th August). No further actors from the initial list have appeared since then suggesting a certain level of network stability. We will discuss this in more detail in our analysis below.

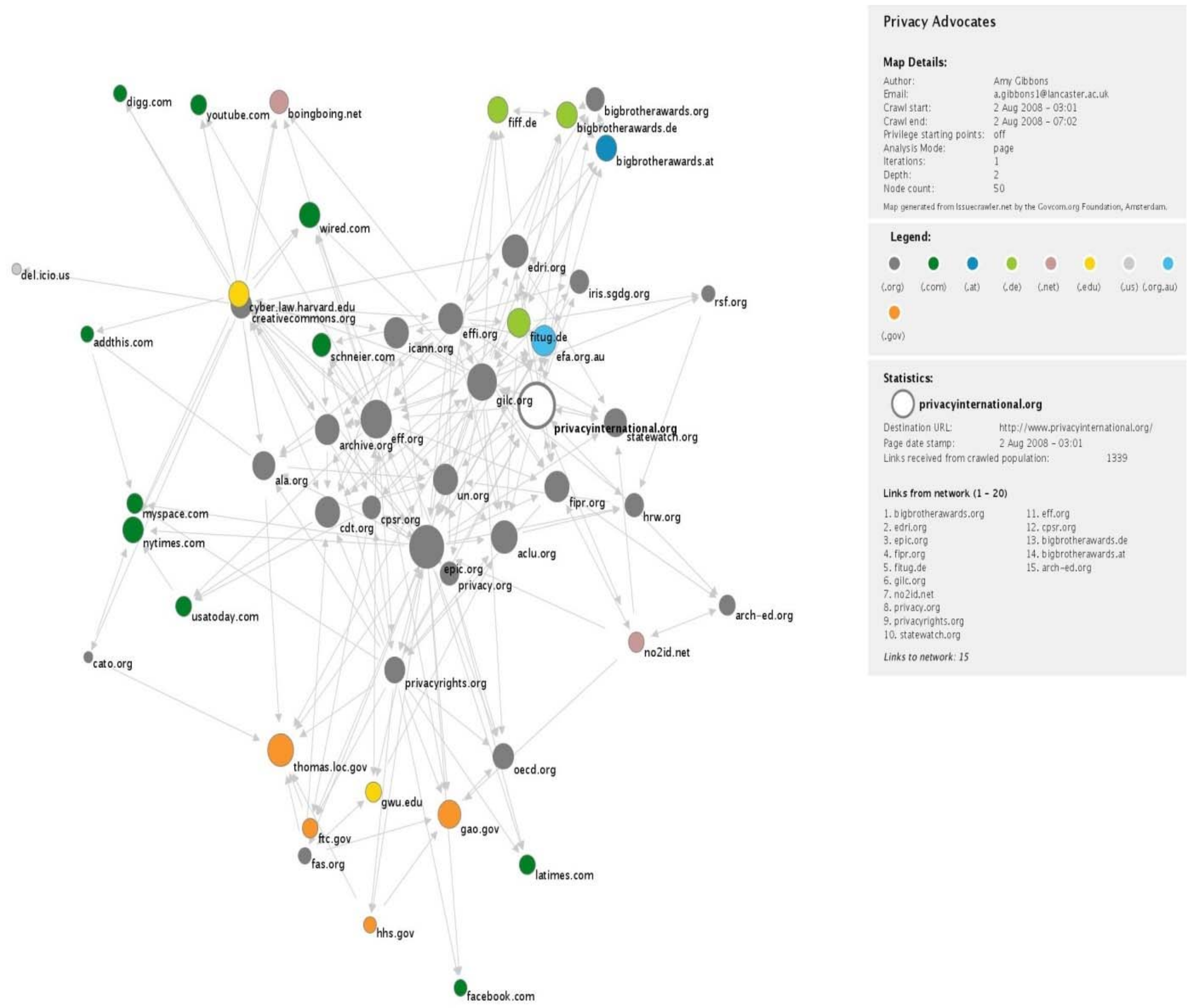
In order to understand how the actors, who are members of the network, relate we need to do some further analysis. These interrelationships can be represented through a number of SNA metrices such as density, centrality, clusters, bridges, and so forth. In this paper we will not do a complete SNA (this is beyond the scope of the paper). Rather we will use sociograms generated by *IssueCrawler* to provide an initial representation of the interrelationships of the network. We must keep in mind that a crawl is in a sense a 'snapshot' of the network at particular point in time. For example if we look as Figure 1 (the sociogram for the crawl of the 2nd of August 2008) we can note the following. First, in these diagrams the *centrality* of an actor is indicated by the relative size of the circle in the diagram. The centrality of the actor is a direct reflection of their link density (or influence one might say) within the network both internally and externally to other actors. In Figure 1 privacyinternational.org is indicated as the most central actor in the network. Second, *IssueCrawler* categorises actors according to top-level domain name. For example in Figure 1 all .org sites are indicated in grey and all .com sites are indicated in green. Unfortunately the user does not control this categorisation process. Third, in the diagram we see which actors are connected with which other actors (given a certain density threshold). These links also indicate direction. In the diagram we see a list of actors below the heading "*Links from the network*". These are actors who received links from the actors in the network and those below the heading "*Links to the network*" are those actors who link to other actors in the network.[23] As mentioned earlier, a complete listing of the actors (based on their domain name as indicated in the sociogram) is provided in *Appendix 2*. With this basic information to hand we can now do an analysis of the different crawls from *IssueCrawler*, as indicated below.

A tentative analysis of some network crawls

Let us first consider the sociogram that resulted from the network crawl of the 2nd of August 2008 (indicated in Figure 1). We first note that privacyinternational.org is the most central actor. This is not surprising given the prominence of the actor in a variety of campaigns against state surveillance (such as the ID card campaign for example).[24] Other significant actors are, for example, the Electronic Privacy Information Centre (epic.org), the Electronic Frontier Foundation (eff.org) and statewatch.org. All of these are to be expected. Some more unexpected actors (in terms of prominence) are European Digital Rights (edri.org), the Foundation for Information Policy Research (fipr.org) and the United Nations (un.org).

[23] More information on the structure of the maps can be found on the *IssueCrawler* FAQ site: http://wiki.issuecrawler.net/Issuecrawler/FAQ#What_are_links_from_the_network (accessed November 2, 2008)

[24] Privacy International have conducted a series of studies into this area and in 2004 produced an interim report entitled *'Mistaken Identity; Exploring the Relationship Between National Identity Cards & the Prevention of Terrorism'*. http://www.privacyinternational.org/issues/idcard/uk/id-terrorism.pdf (accessed November 3, 2008)



Privacy Advocates

Map Details:

Author:	Amy Gibbons
Email:	a.gibbons1@lancaster.ac.uk
Crawl start:	2 Aug 2008 - 03:01
Crawl end:	2 Aug 2008 - 07:02
Privilege starting points:	off
Analysis Mode:	page
Iterations:	1
Depth:	2
Node count:	50

Map generated from Issuecrawler.net by the Govcom.org Foundation, Amsterdam.

Legend:

Statistics:

○ **privacyinternational.org**

Destination URL:	http://www.privacyinternational.org/
Page date stamp:	2 Aug 2008 - 03:01
Links received from crawled population:	1339

Links from network (1 - 20)

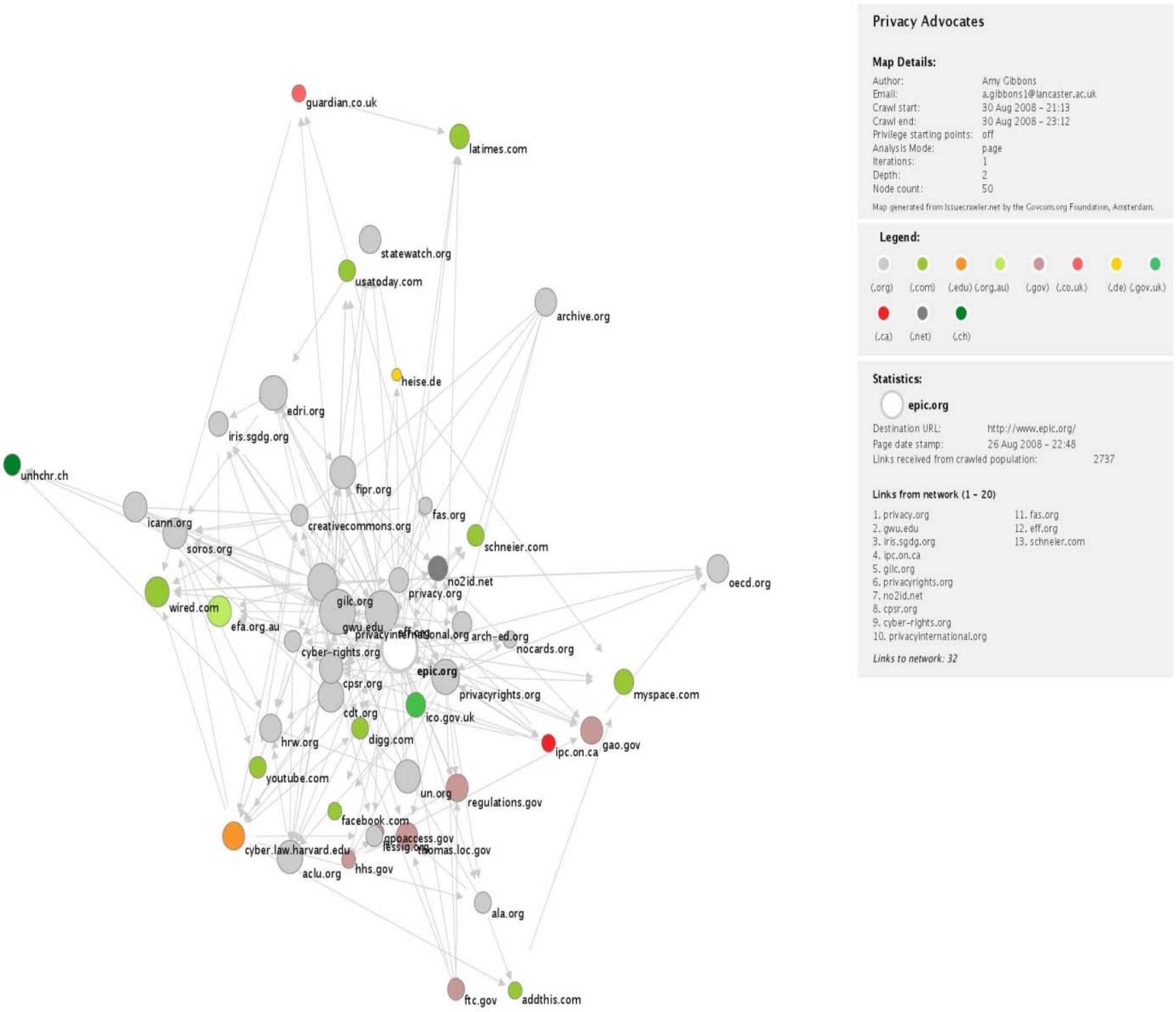
1. bigbrotherawards.org
2. edri.org
3. epic.org
4. fipr.org
5. fitug.de
6. gilc.org
7. no2id.net
8. privacy.org
9. privacyrights.org
10. statewatch.org
11. eff.org
12. cpsr.org
13. bigbrotherawards.de
14. bigbrotherawards.at
15. arch-ed.org

Links to network: 15

Figure 1: **Sociogram – 2 August 2008**

From the diagram (and the 'links to' and the 'links from' lists) it seems that there is a high level of co-linking (i.e. cohesiveness) between the advocacy sub-networks (designated with the .org domain). In contrast the co-linking between advocacy groups and the traditional media is relatively lower than one would have expected. Linking from advocacy groups to the traditional media would probably be driven by reporting around specific incidents. The lack of linking from traditional media to advocacy groups (with the exception of Wired Magazine) might be because the traditional media see new media as competition. Given the prominence of the traditional media (especially for the off-line audience) it seems important that the advocacy groups find a way to cultivate co-linking relationships with the traditional media in order to draw them into the network.

Another interesting feature of the network is the relationship between advocacy groups and social media (such as MySpace, Facebook, YouTube, etc.). There again seems to be limited co-linking between advocacy actors and social media. One would expect that since this media is not subject to the same editorial and journalistic control that there would be a much higher level of co-linking. There are a number of other interesting observations one might make with regard to this particular diagram. We will pick some of these up as we discuss subsequent diagrams.



Privacy Advocates

Map Details:

Author:	Amy Gibbons
Email:	a.gibbons1@lancaster.ac.uk
Crawl start:	30 Aug 2008 – 21:13
Crawl end:	30 Aug 2008 – 23:12
Privilege starting points:	off
Analysis Mode:	page
Iterations:	1
Depth:	2
Node count:	50

Map generated from Issuecrawler.net by the Govcom.org Foundation, Amsterdam.

Legend:

● (.org) ● (.com) ● (.edu) ● (.org.au) ● (.gov) ● (.co.uk) ● (.de) ● (.gov.uk)

● (.ca) ● (.net) ● (.ch)

Statistics:

○ **epic.org**

Destination URL:	http://www.epic.org/
Page date stamp:	26 Aug 2008 – 22:48
Links received from crawled population:	2737

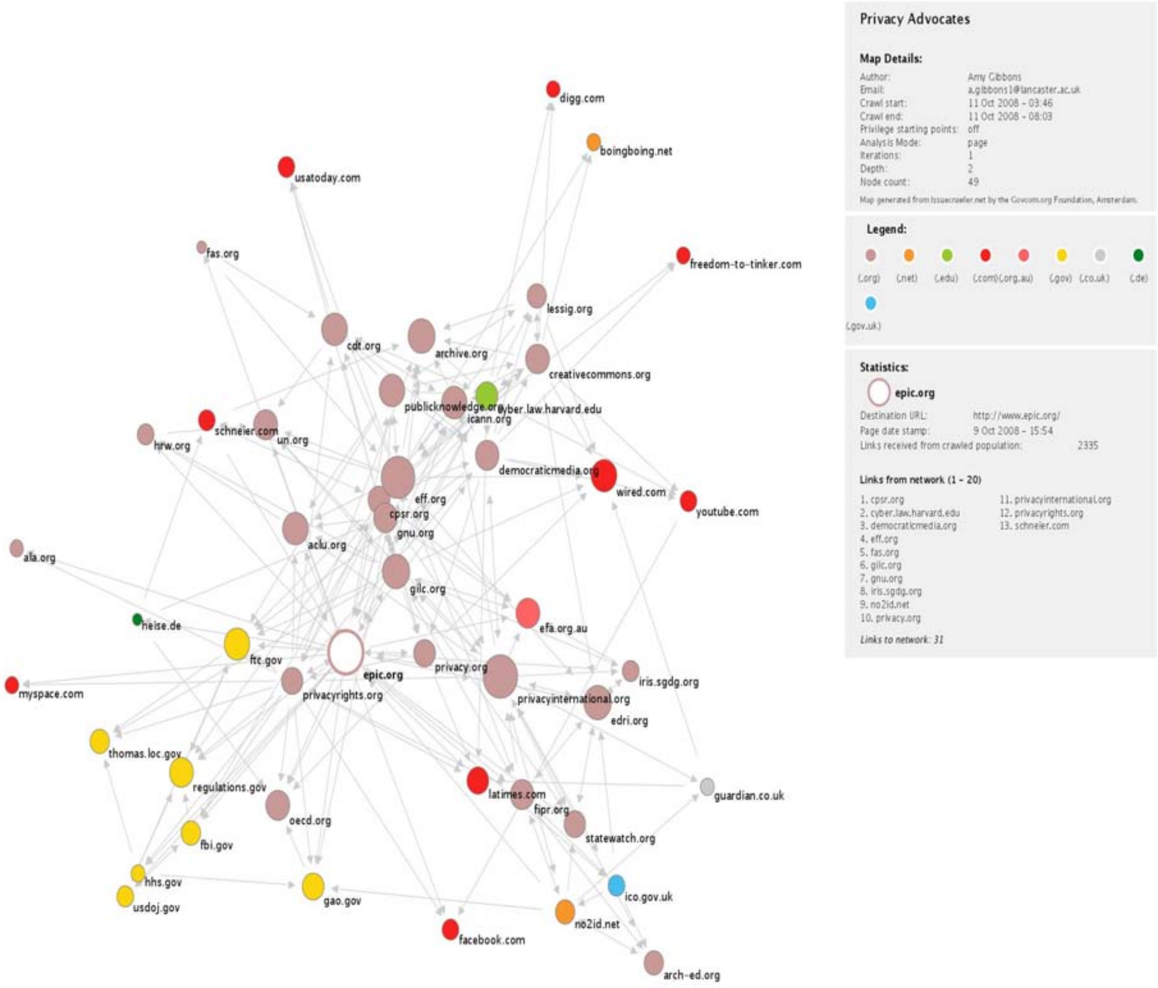
Links from network (1 - 20)

1. privacy.org
2. gwu.edu
3. iris.sgdg.org
4. ipc.on.ca
5. gilc.org
6. privacyrights.org
7. no2id.net
8. cpsr.org
9. cyber-rights.org
10. privacyinternational.org
11. fas.org
12. eff.org
13. schneier.com

Links to network: 32

Figure 2: **Sociogram - 30th August 2008**

The network crawl of 30th of August 2008 (indicated in Figure 2) is perhaps one of the more interesting sociogram of the crawls so far, as noted by the higher density of advocacy organisations (depicted by the light grey circles in this diagram). A prominent actor, which had not featured in the network previously, was the UK based Guardian newspaper. At the time that the crawl was conducted newspapers in the UK had reported on two major data protection incidents. The first of these were government discs containing the names of thousands of convicted criminals and discussions centred on compensation. The second was yet another incident of data being on a stolen laptop computer. It seems that this is just the tip of the iceberg in the number of similar incidents, which seem to have become media fodder in recent months. Undoubtedly the catalyst for the media interest was the widely condemned loss of computer discs by Her Majesty's Revenue and Custom's (HMRC) office containing the details of every child benefit claimant including personal data such as address, name and child's name. The discs, which have not yet been recovered, were lost in transit and had been given to a junior employee to send by mail service. The data on the discs were not encrypted. This sparked a national outcry into the safety of data stored by government institutions and even the Information Commissioner capitalized on the opportunity to stress the need for tighter security measures.



Privacy Advocates

Map Details:

Author:	Amy Gibbons
Email:	a.gibbons1@lancaster.ac.uk
Crawl start:	11 Oct 2008 - 03:46
Crawl end:	11 Oct 2008 - 08:03
Privilege starting points:	off
Analysis Mode:	page
Iterations:	1
Depth:	2
Node count:	49

Map generated from Issuecrawler.net by the Govcom.org Foundation, Amsterdam.

Statistics:

epic.org

Destination URL:	http://www.epic.org/
Page date stamp:	9 Oct 2008 - 15:54
Links received from crawled population:	2335

Links from network (1 - 20)

1. cpsr.org
2. cyber.law.harvard.edu
3. democraticmedia.org
4. eff.org
5. fas.org
6. gilc.org
7. gnu.org
8. iris.sgdg.org
9. no2id.net
10. privacy.org
11. privacyinternational.org
12. privacyrights.org
13. schneier.com

Links to network: 31

***Figure 3:* 11th October Sociogram**

As we develop our methodology we would want to track major incidents through the network. This means that we would need to collect data on a sufficiently regular basis or use the *Internet Archive*[25] as a source (although this might be somewhat problematic since the archive appears to store information almost two months after it had originally been posted).

If we look at Figure 2 we also see the Ontario Office of the Information and Privacy Commissioner (ipc.on.ca) and the Information Commissioner's Office of the UK (ico.gov.uk) included in the network. These are independent 'watchdog' organisations that are there to ensure that the rights of individuals are protected. The co-linking between them and the advocacy organisations are interesting since one might argue that they can act as possible intermediaries for information flow between the advocacy groups and state institutions.

[25] http://www.archive.org/index.php

The sociogram of 11th October 2008 (in Figure 3) highlighted a strong state presence in the network. Two, out of the three new actors that appeared in the network were classified as state actors; the UK Ministry of Justice (justice.gov.uk) and the US Department of Justice (us.doj.gov). In some cases, *IssueCrawler* retrieves the exact URL that was being linked to within the network. This is not always possible and in these instances only the home page of the site is given. In this network, however, there were a number of specific links, mainly on government and news web pages. The central issue around this time appears to be ID cards, predominantly in the United Kingdom (UK) and in the United States of America (USA).

This is the issue that appears dominant, due to the unusual retrieval of several direct links and therefore we are making a supposition that the overall intentionality of the network that day was to inform the public about ID cards, at a time when it was being discussed publicly. To further support that claim we researched the issues around the time and a simple Google search demonstrated the publicity of the ID cards *issue*, in August, so it is not surprising that this was linked to by several advocate sites.[26] The most highly ranked of these was the EPIC National and Real ID Act, which also appeared in the network (as seen in Figure 3). A couple of examples of specific sites that were returned, which were made visible by *IssueCrawler*, were Realnightmare.org's page on Anti-Real ID Legislation in the States[27] and EPIC's National ID Cards and Real ID Act[28] and both the Federal Trade Commission's and Ministry of Defence offering guidelines on how to fight back against ID theft.[29] Interestingly a story from the USA Today on an NSA call database, which appeared in the 30th August crawl, a date when the network was unusually shifted towards advocacy sites, was also retrieved in this crawl.[30] Again, as we develop our methodology we would want to track issues in the way they reconfigure the network relationships (both temporarily and over a period of time).

Other aspects of the network's linking patterns

In this sub-section we will explore some further features of the network and discuss the way in which these may add to or detract from the network becoming a cohesive, global network on issues of surveillance and privacy.

The periphery. As previously stated, the page and site analyses that *IssueCrawler* provides are only the details of reciprocal links between actors. We were also interested to establish the actors which were on the periphery (those who are linked to but do not return a link to the host site). In order to do this we exported all the raw data to an affiliate application called *UCINet*. We were then able to view all the links in the network and cross compare the list of actors *IssueCrawler* had retrieved against the whole list, those that remained were the periphery actors. A total of 68 actors were classed as peripheral, over the course of all the crawls we conducted between the 2nd August and 8th November 2008. Some of these have had reciprocal relationships in the network and as such have only appeared on the periphery a small number of times. We were particularly interested in the actors who have not yet been recognised by the core. Twenty six (26) of the actors, in the periphery, were in the initial list of actors we categorised as privacy advocates, including actors such as NSA Watch, the Surveillance Studies Network, ALCEI (Electronic Frontiers, Italy) and Wikileaks. The first three appeared in all 9 crawls and Wikileaks appeared in 8. It is

[26] Examples include 'ID Plan in Crisis after Guinea Pig Workers Revolt' http://www.guardian.co.uk/politics/2008/oct/12/idcards (accessed November 3, 2008), the Independent's Letter's page http://www.independent.co.uk/opinion/letters/letters-id-cards-954482.html (accessed 3 November, 2008) and biometric fingerprinting in US schools http://www.cr80news.com/2008/08/18/schools-replacing-photo-id-cards-with-biometrics (accessed November 3, 2008)

[27] See http://www.realnightmare.org/news/105; http://www.gwu.edu/~nsarchiv: Anti-Real ID Legislation in the States http://www.justice.gov.uk/reviews/datasharing-intro.htm (accessed November 3, 2008)

[28] See http://epic.org/privacy/id-cards (accessed November 3, 2008)

[29] See http://www.ftc.gov/bcp/edu/microsites/idtheft/ (accessed November 3, 2008)

[30] http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm (accessed November 2, 2008)

therefore puzzling why these actors have not yet received links from the core (i.e. not appeared in any of the sociograms). Why are the actors in the core not linking to them? Clearly it would be in the interest of the network to draw these relevant actors into the core. This would reduce the degrees of separation and add to the value of the entire network, thereby increasing the probability that the network can become a more effective vehicle for information politics, meta-surveillance and possibly resistance.

Affiliate actors. Many of the sites in the network are specific information sites set up by advocate groups. Others are collaborations between advocacy groups, demonstrating an acknowledgment of the mutual benefits available to the network of sharing information, knowledge and expertise. Examples include dataretentionisnosolution.com, a petition site against the plans of the UK government to store all telephone and internet traffic data. This site was set up by Digital Civil Rights in Europe (EDRI) in 2005 and we may well see a revival of the site in the network given the current prominence of this issue in the UK media. Other examples include tor.eff.org (a software project to defend against traffic analysis), spychips.com (petitioning against the use of RFID) and realnightmare.org (campaigning against the Real ID Act of 2005), affiliates of the EFF, CASPIAN and the ACLU respectively.

What is interesting to note is that because these affiliate actors feature independently in the network they are afforded a more influential status, within the network as a whole, since they are accessible from multiple points within the network—i.e. there are less degrees of freedom to get to them from the core. It seems that the cultivation of links through affiliate actors has the potential to strengthen the position of the core actors in the network. It will also strengthen the position of sites in the periphery that they may link to.

Geography. *IssueCrawler* has a series of affiliated tools for analytical purposes. One of these tools is Issue Geographer, which returns a geographic analysis of actors' base locations in the *real* world (based on where the domain name is registered, which is obviously not entirely accurate). In conjunction with the tool (on average the tool only returns approximately a fifth of the base locations in this network) we conducted an online analysis of the actors' base locations and found the following results:

> Amsterdam (1); Australia (1); Austria (2); Belgium (5); California (15); Finland (1); France (3); Germany (6); Illinois (3), Massachusetts (2); New Jersey (2); New York (10); Ontario (2); Portugal (1); Rhode Island (2); Switzerland (1); Tennessee (1); UK (20); unknown (14); US (3) (state unknown) Virginia (6); Washington (1) Washington DC (25); Wyoming (1).

The data indicates a strong western bias (indeed North America (55%) and UK (16%) bias), which could be for a number of reasons. There could be a language barrier between English and non-English speaking sites, legislation in certain countries may restrict freedom of speech or there may be actors who, out of a desire to remain anonymous, would mask their location. Of course, statistically North America and Europe are higher overall users of the Internet[31] than the other areas mentioned. Nevertheless, this is an issue that the advocacy network may want to consider.

Some conclusions and future work

The aim of this paper was to do an initial exploration as to whether the actors concerned with state surveillance can be said to constitute a network of resistance through the mechanisms of information politics and meta-surveillance. It was argued that such a network based on the mechanisms of information politics and meta-surveillance might be the one of the effective means for citizen to resist state surveillance. The question then becomes one of whether such a network exists and to what extent it is (or can be) a coherent and cohesive system for information politics and meta-surveillance? In order to

[31] http://www.internetworldstats.com/stats.htm (accessed November 3 2008)

evaluate such a proposition we used the principles of social network analysis and the small world hypothesis, as well as a variety of web-based tools to perform a webometric network analysis of the advocacy network. The intention was to establish if there was indeed a network and what the characteristics of such a network would be. From our data collection and analysis we can provide the following tentative conclusions.

- There seems to be a relatively stable network of core actors. These are the actors one would expect to find such as Privacy International (privacyinternational.org), Electronic Privacy Information Centre (epic.org), the Electronic Frontier Foundation (eff.org) and Statewatch.org. However, there are a number of important actors that seem to remain on the periphery of the network. This seems to detract from the potential of the network to become an effective system for information politics and meta-surveillance.
- The density of the network is relatively low. This means that there is a relatively low level of reciprocal linking between all the actors in the network. Reciprocal linking draws actors into the network (i.e. reduces the degrees of separation) and increases the positive network externalities for all the actors in the network.
- It seems that the network is not yet able to effectively link to the traditional or new media as intermediaries. Enrolling the traditional media as well as the new media into the network (at least around certain important events) is important for the 'reach' of the network, and is especially important for effective information politics.
- The network is highly biased and skewed towards the west (North America and the UK in particular). This must clearly be a matter of concern since state surveillance practices are increasingly global.

Our overall, and tentative, conclusion would be that the advocacy network still seems somewhat fragmented with a relatively small, and geographically biased, core. This seems to concur with Bennett's (2008) claim that the advocacy network is "dynamic, volatile, overlapping, fragmented and somewhat elusive," without a clear structure, nor an identifiable base. However, it could be argued—from the point of network theory—that the network will be more effective in its information politics if it is more cohesive, at least in the way it links to each other in the online environment. By reducing the degrees of separation the network can foster links between different data sets, create links between information about incidents, corroborate information (making it more credible), and so forth. This is especially true if the network can succeed to enrol important intermediaries such as the traditional media, the new social media, commissioners, researchers, etc. into the network. If successful it might ultimately become a network of meta-surveillance that has the potential to transcend the individual actor's agency into a system of collective awareness of state-surveillance practices. Such collective awareness can most certainly become a powerful form of resistance. On the other hand it might be argued that it is important to the survival of the network that it remains 'dynamic, volatile, overlapping, fragmented and somewhat elusive' (as suggested by Bennett, 2008); a network of loosely connected centres that might be more resilient and able to resist attempts to counteract its activities. This is an issue to explore with the actors involved in subsequent qualitative interviews.

As mentioned before, this is an ongoing research project. We acknowledge that there is a limit to what one might be able to conclude from the type of link data that we have collected. The issues mentioned above are best explained by the actors themselves, in order to perform a more comparative analysis between the *online* activities and *offline* activities. It would also be interesting to see the role that the actors consider themselves to play in this online environment, especially with regard to their intentions in relation to the network as a whole. We intend to conduct a series of qualitative interviews, with the actors in the network. The results of our network analysis will be shown to each of the actors, including their individual data and how they are positioned in the broader network.

However, in order to make the support for our hypothesis more robust we believe we need to triangulate our network analysis and qualitative interviews with a third data set. We would suggest that to form a true representation of the network effects we need to make transparent all links which are being made to the network actors, not just the visible ones (the online hyperlinks, public reporting and campaigning) but also the invisible ones. Analysing traffic log data and the IP addresses of visitors to the advocacy network's sites will fulfil this function. This will give us a more comprehensive indication of reciprocity between non-state and state actors and the extent to which the network is effective in its information politics and its overall intention to resist state surveillance. This paper is a tentative step towards a better understanding of the potential of the new media to develop a system of meta-surveillance as an organic and continually emerging mode of resistance to state surveillance. We believe it has made a start towards such an understanding but much more needs to be done.

Acknowledgements

We would like to thank the reviewers and editors for their thoughtful comments and suggestions.

References

American Civil Liberties Union. 2003. *Bigger Monster, Weaker Chains.* ACLU Technology and Liberty Program.

American Civil Liberties Union. 2007a. *Even Bigger, Even Weaker: The Emerging Surveillance Society: Where Are We Now?* ACLU Technology and Liberty Program.

American Civil Liberties Union. 2007b. *What's wrong with Fusion Centres?* ACLU Technology and Liberty Program.

Adamic, L. and Glance, N. 2005. The political blogosphere and the 2004 U.S. election: Divided they blog. http://www.blogpulse.com/papers/2005/AdamicGlanceBlogWWW.pdf [accessed March 10, 2008]

Adamic, L. A., & Adar, E. 2001. You are what you link. *Paper presented to the 10th annual International World Wide Web Conference*, Hong Kong. http://www10.org/program/society/yawyl/YouAreWhatYouLink.htm [accessed November 11, 2008]

Barabási, A. L. 2002. *Linked: The New Science of Networks.* Cambridge*:* Perseus Publishing.

Bennett, C. 2008. *The Privacy Advocates: Resisting the spread of surveillance*. Cambridge: MIT Press.

Borgatti, S., Everett, M. G. and Freeman, L. C. 2002. *Ucinet for Windows: Software for Social Network Analysis.* Harvard, MA: Analytic Technologies.

Broder, A.K.R., Maghoul, F., Raghavan, P., Rajagopalan, S., Stata, R., Tomkins, A. & Wiener, J. 2000. Graph structure in the Web. *Journal of Computer Networks* 33(1-6): 309-320.

Buchanan, M. 2002. *Nexus: Small Worlds and the Groundbreaking Science of Networks.* London: W.W. Norton & Company.

Ciborra, C. 2002. *The Labyrinths of Information: Challenging the Wisdom of Systems*. Oxford: Oxford University Press.

Clarke R., 1994. The digital persona and its application to data surveillance. *The Information Society* 10(2): 77 – 92.

Courtois, M. P. and Berry, M. W. 1999. Results ranking in web search engines. *Online* 23 (3): 39-46.

Crossman, G. 2007. *Overlooked: Surveillance and Personal Privacy in Modern Britain.* London: Liberty.

EC Commission. 2000. The Commission and Non-Governmental Organisations: Building a Stronger Partnership. Commission Discussion Paper http://ec.europa.eu/civil_society/ngo/index_en.htm [accessed November 11, 2008]

Foot, K.A. et al 2003. Analyzing linking practices: candidate sites in the 2002 US electoral web sphere. *Journal of Computer-Mediated Communication* 8(4) http://jcmc.indiana.edu/vol8/issue4/foot.html [accessed March 10, 2008]

Freeman, L. C. 2004. *The Development of Social Network Analysis: A Study in the Sociology of Science.* Vancouver: Empirical Press.

Garrido, M. and Halavais, A. 2003. Mapping networks of support for the Zapatista movement: applying social-networks analysis to study contemporary social movements. In M.McCaughey and M.D. Ayers (eds). *Cyberactivism: Online Activism in Theory and Practice*. 165-84. London: Routledge.

Garton, L., Haythornthwaite, C. and Wellman, B. 1997. Studying online In Lancaster, F.Wilfred. and Lee, Ja-Lih. 1985. Bibliometric techniques applied to issue management: a case study. *Journal of the American Society for Information Science.* 36(6): 389-397.

Gordon, Colin. 1980. (eds.) *Michel Foucault: Power/Knowledge: Selected Interviews and Other Writings 1972-1977.* London: Harvester.

Haggerty, K. and Ericson, R.V. 2006. *The New Politics of Surveillance and Visibility*. London: University of Toronto Press.

Hargittai, E. 2007. Whose space? Differences among users and non-users of social network sites. *Journal of Computer-Mediated Communication* 13(1) http://jcmc.indiana.edu/vol13/issue1/hargittai.html [accessed March 10, 2008]

Hawking, D et al. 2001. Measuring search engine quality. *Information Retrieval*. 4(1): 33-59.

Hsu, C-L 2008. *Revealing Virtual Political Networks: A Webometric Analysis of the Taiwanese Pro-Independence Movement*, unpublished PhD thesis, Lancaster University.

Introna, L. D. & Nissenbaum, H. 2000. Shaping the Web: Why the Politics of Search Engines Matter. *The Information Society* 16(3): 169-185.

Keck, M.E and Sikkink, K. 1998. *Activists beyond borders: advocacy networks in international politics.* New York: Cornell University Press.

Kerr, I., Forcese, C., Jackman, B., Lyon, D. and Stoddart, J. 2007. *In: National Security, Surveillance Technology and Human Rights in Canada.* 19th September 2007, Law and Technology, University of Ottawa, Canada.

Krotoszynski Jr, R.J. 1990. Autonomy, Community and Traditions of Liberty: The Contrast of British and American Privacy Law. *Duke Law Journal 6*: 1398-1454.

Liberty 2007. Britain's Privacy – Casualty in the War on Terror? YouGov poll. http://www.liberty-human-rights.org.uk/news-and-events/1-press-releases/2007/britain-s-privacy.shtml [accessed 1 November, 2008]

Lin, J. and Halavais, A. 2004. *Mapping the blogosphere in America.* http://www.blogpulse.com/papers/www2004linhalavais.pdf [accessed March 12, 2008]

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

Nooy, W., Mrvar, A. and Batageli, V. 2005. *Exploratory Social Network Analysis with Pajek.* Cambridge: Cambridge University Press.

Park, H. & Thelwall, M. 2003. Hyperlink analyses of the world wide web: A review. *Journal of Computer-Mediated Communication* 8(4). http://jcmc.indiana.edu/vol8/issue4/park.html [accessed March 12, 2008]

Privacy International. 2007. Leading Surveillance Societies in Europe and the World 2007 http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597 [accessed May 21, 2008]

Raab, C, D. 2003. Joined-up Surveillance: The Challenge to Privacy. In. Ball, K. and Webster F. (eds). *The Intensification of Surveillance.* London: Pluto Press

Rogers, R. 2004. *Information Politics on the Web*. Cambridge: MIT Press

Rogers, R. and Marres, N. 2000. Landscaping climate change: a mapping technique for understanding science and technology debates on the world wide web. *Public Understanding of Science* 9(2): 141-163.

Suchman, L. 1994. Do Categories Have Politics? The Language/action perspective reconsidered. *Computer Supported Cooperative Work (CSCW)* **2**(3): 177-190

Surveillance Studies Network. 2006. 'A Report on the Surveillance Society'. http://www.ico.gov.uk/.../library/data_protection/practical_application/surveillance_society_full_report_2006.pdf (accessed February 20, 2008)

Tavani, H.T. 1999. KDD, Data Mining, and the Challenge for Normative Privacy. *Ethics and Information Technology* 1(4): 265-273

Thelwall, M. 2007a. Blog searching: the first general-purpose source of retrospective public opinion in the social science? *Online Information Review* 31(3):277-289.

Thelwall, M. 2007b. *Social networks, fender and friending: an Analysis of MySpace member profiles.* http://www.scit.wlv.ac.uk/~cm1993/papers/MySpace_d.doc [accessed March 13, 2008]

Thelwall, M. and Hellsten, I. 2006. The BBC, *Daily Telegraph* and Wikinews timelines of the terrorist attacks of 7th July 2006 in London: a comparison with contemporary discussions. *Information Research* 12(1). http://InformationR.net/ir/12-1/paper284.html [accessed March 13, 2008]

Thelwall, M. and Stuart, D. 2006. Web Crawling Ethics Revisited: Cost, Privacy and Denial of Service. *Journal of American Society for Information Science and Technology* 57(13): 1771-1779.

Thelwall, M. & Wilkinson, D. 2003. Graph structure in three national academic Webs: Power laws with anomalies. *Journal of the American Society for Information Science and Technology* 54(8): 706-712.

Thelwall, M. 2002. In praise of Google: finding law journal web sites. *Online Information Review.* 26(4):271-272.

Thelwall, M. 2000. Web impact factors and search engine coverage. *Journal of Documentation* 56(2):185-189.

Urry, J. 2007. *Mobilities.* Cambridge: Polity

Van den Bos, M. 2006. Hyperlinked Dutch-Iranian cyberspace. *International Sociology* 21(1): 83-99.

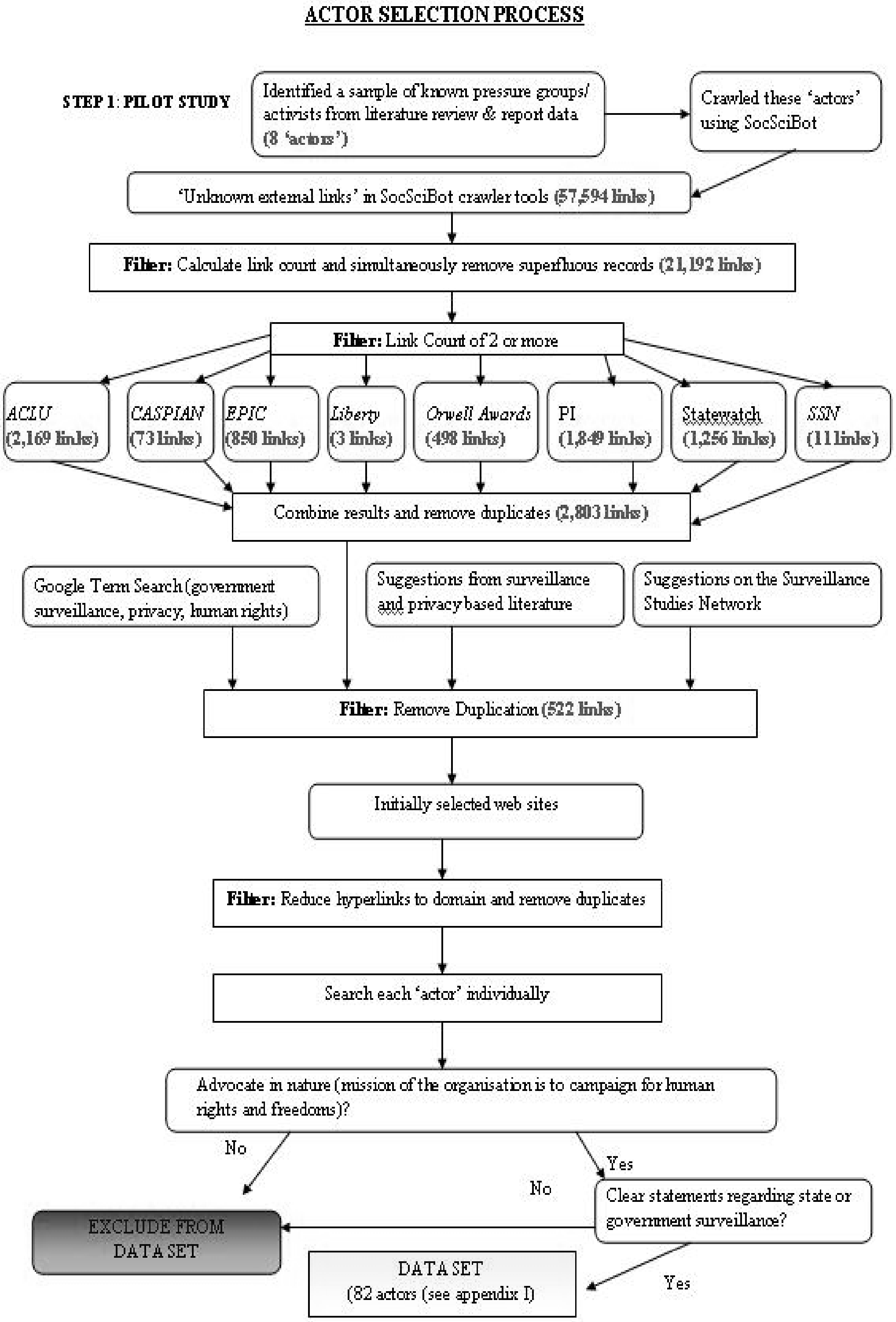
Vaughan, L. and Thelwall, M. 2004. Search engine coverage bias: evidence and possible causes. *Information Processing and Management* 40(4): 693-707.

Watts, D.J. 2003. *Six Degrees: The Sciences of a Connected Age.* London: The Random House Group Limited

Winograd, T. 1994. Categories, Discipline and Social Co-ordination. *Computer Supported Cooperative Work* 2(3): 191-197

Wormell, I. 2000. Critical aspects of the Danish welfare state – as revealed by issue tracking. *Scientometrics* 48(2): 237-250.

Appendix I: The Actor Selection Process


ACTOR SELECTION PROCESS
STEP 1: PILOT STUDY
Identified a sample of known pressure groups/ activists from literature review & report data (8 'actors')
Crawled these 'actors' using SocSciBot
'Unknown external links' in SocSciBot crawler tools (57,594 links)
Filter: Calculate link count and simultaneously remove superfluous records (21,192 links)
Filter: Link Count of 2 or more
ACLU (2,169 links)
CASPIAN (73 links)
EPIC (850 links)
Liberty (3 links)
Orwell Awards (498 links)
PI (1,849 links)
Statewatch (1,256 links)
SSN (11 links)
Combine results and remove duplicates (2,803 links)
Google Term Search (government surveillance, privacy, human rights)
Suggestions from surveillance and privacy based literature
Suggestions on the Surveillance Studies Network
Filter: Remove Duplication (522 links)
Initially selected web sites
Filter: Reduce hyperlinks to domain and remove duplicates
Search each 'actor' individually
Advocate in nature (mission of the organisation is to campaign for human rights and freedoms)?
No
Yes
No
Clear statements regarding state or government surveillance?
EXCLUDE FROM DATA SET
DATA SET (82 actors (see appendix I)
Yes

Appendix II: Details of the Network Actors

Please note that the descriptions used below are based on the taglines of the websites, not on the opinions of the authors. The location and contact details are a rough approximation of the location of the actors. Categories are used to demonstrate the range of actors in the network. The *IssueCrawler* application categorises the actors based on domain name for example .org or .com. Please note that by categorizing an actor as an advocate in this table we are not implying that the actor is a privacy advocate. Several actors that appear in the network are primarily campaigning for other human rights and fundamental freedoms for example abolition of the death penalty.

Web Addresses of Actors	Full Name and Description of Actor	Category (NSA = Non State Actor/ SA = State Actor)	Date Joined Network	Location
abcnews.go.com	ABC News	News/Media (NSA)	25/10/2008	California
accessreports.com	Access Reports, Freedom of Information Act and Privacy Issues	Privacy Advocate and News/Media (NSA)	02/08/2008	Lynchburg, Virginia
aclu.org	American Civil Liberties Union	Advocate (NSA)	02/08/2008	New York, New York
acm.org	Association for Computing Machinery	Education (NSA)	02/08/2008	New York, New York
addthis.com	AddThis – Social Networking Site	Social Networking Site (NSA)	02/08/2008	Princeton, New Jersey
ael.be	Association Electronique Libre (AEL)	Advocate (NSA)	16/08/2008	Wanze, Belgium
aktiv.org	Adult Search Engine	Adult Website (NSA)	25/10/2008	Unknown
ala.org	American Library Association	Reference (NSA)	02/08/2008	Chicago, Illinois
amnesty.org	Amnesty International	Advocate (NSA)	02/08/2008	London, UK
andrebacard.com	Author André Bacard's "Facts, Fables & Foibles"	Education (NSA)	02/08/2008	Only listed e-mail address
anonymizer.com	Anonymizer: Anonymous Web Surfing	Commercial (NSA)	02/08/2008	San Diego, California
apecsec.org.sg	Apecsec: Conflict Resolution Resource	Reference (NSA)	02/08/2008	Only listed e-mail address
arch-ed.org	Action on Rights for Children	Advocate (NSA)	02/08/2008	London, UK
archive.org	Internet Archive	Reference (NSA)	02/08/2008	San Francisco
article19.org	Article 19: Global Campaign for Free Expression	Advocate (NSA)	02/08/2008	London, UK
ask.com	Ask.com: Search Engine	Search Engine (NSA)	16/08/2008	London, UK
bigbrotherawards.at	Big Brother Awards Austria 2008	Advocate (NSA)	02/08/2008	Wien, Austria
bigbrotherawards.de	Big Brother Awards Germany	Advocate (NSA)	02/08/2008	Bielefeld, Germany

bigbrotherawards.eu.org	Big Brother Awards Europe (quintessenz)	Advocate (NSA)	16/08/2008	Paris, France
bigbrotherawards.org	Big Brother Awards International	Advocate (NSA)	02/08/2008	Vienna, Austria
bof.nl	Bits of Freedom	Advocate (NSA)	02/08/2008	Amsterdam
boingboing.net	Boing Boing: A Directory of Wonderful Things	Blog (NSA)	02/08/2008	Sherman Oaks, California
cato.org	The CATO Institute	Research (NSA)	02/08/2008	Washington, DC
cauce.org	Coalition Against Unsoliticed Commerical Email	Advocate (NSA)	02/08/2008	Trumsburg, New York
ccc.de	Chaos Computer Club e.V.	Advocate (NSA)	16/08/2008	Berlin, Germany
cdt.org	Centre for Democracy and Technology	Education and Advocate (NSA)	02/08/2008	Washington DC
cfoi.org.uk	Campaign for Freedom of Information	Advocate (NSA)	02/08/2008	London, UK
cfp2005.org	Computers Freedom and Privacy Conference 2005	Research (NSA)	02/08/2008	Seattle – location changed to Washington DC for 2009
cippic.ca	Canadian Internet Policy and Public Interest Clinic	Educational (NSA)	25/10/2008	Ottawa, Ontario
cme.org	The Christian Methodist Episcopal	Religious (NSA)	30/08/2008	Memphis, Tennessee
commoncause.org	Common Cause: Holding Power Accountable	Advocate (NSA)	08/11/08	Washington D.C
consumer.gov	Consumer.gov: Your resource for consumer information from the federal government	Government Agency (SA)	30/08/2008	e-mail address only
consumer-action.org	Consumer Action	Advocacy and Education (NSA)	02/08/2008	Washington DC
consumerfed.org	Consumer Federation of America	Advocate and Research (NSA)	30/08/2008	Washington, DC
cpsr.org	Computer Professionals for Social Responsibility	Advocate (NSA)	02/08/2008	Stanford, California
cptech.org	Consumer Project on Technology	Research (NSA)	02/08/2008	London, UK
craphound.com	Cory Doctorow's Craphound.com	Blog/Advocate (NSA)	11/08/2008	e-mail address only
creativecommons.org	Creative Commons	Charitable Corporation (NSA)	02/08/2008	San Francisco, California
cryptome.org	Cryptome: posts official secrets document to the web, similar in nature to Wikileaks	Advocate (NSA)	16/10/2008	Leeds, UK

cyber.law.harvard.edu	Berkman Centre for Internet & Society at Harvard University	Educational (NSA)	02/08/2008	Cambridge, Massachusetts
cyber-rights.org	Cyber-Rights & Cyber-Liberties: A Non-Profit Civil Liberties Organization	Advocate (NSA)	02/08/2008	Cambridge, Massachusetts
dataretentionisnosolution.com	Data Retention Is No Solution	EDRI	02/08/2008	See EDRI
del.icio.us	Delicious Social Bookmarking	Social Networking Site (NSA)	02/08/2008	Sunnyvale, California
democraticmedia.org	Centre for Digital Democracy	Advocate (NSA)	02/08/2008	Washington, DC
dhs.gov	Department of Homeland Security	State Agency (SA)	11/08/2008	Washington DC
digg.com	Digg: All News, Videos & Images	News/Media (NSA)	02/08/2008	e-mail address only
digitalconsumer.org	DigitalConusmer.org: Protecting fair-use rights in the digital world	Advocate (NSA)	02/08/2008	Madiera, Portugal
edri.org	Digital Civil Rights in Europe	Advocate (NSA)	02/08/2008	Bruxelles, Belgium
efa.org.au	Electronic Frontiers Australia (EFA)	Advocate (NSA)	02/08/2008	North Adelaide, Australia
eff.org	Electronic Frontier Foundation	Advocate (NSA)	02/08/2008	San Francisco, California
effi.org	Electronic Frontier Finland	Advocate (NSA)	02/08/2008	Helsinki, Finland
epic.org	Electronic Privacy Information Centre	Advocate (NSA)	02/08/2008	Washington DC
facebook.com	Facebook	Social Networking Site (NSA)	02/08/2008	Palo Alto, California
fas.org	Federation of American Scientists	Research (NSA)	02/08/2008	Washington, DC
fbi.gov	Federal Bureau of Investigation	Government Agency (SA)	11/10/2008	Washington, DC
fiff.de	Forum InformatikerInnen für Frieden	Advocate/Blog (NSA)	02/08/2008	Bremen, Germany
fipr.org	Foundation for Information Policy Research	Research (NSA)	02/08/2008	Cambridge, UK
fitug.de	FITUG e.V. Förderverein Informationstechnik und Gesellschaft	EDRI (NSA)	02/08/2008	Jena, Germany
freedominfo.org	Freedominfo.org: The Online Network of Freedom of Information Advocates	Advocate (NSA)	02/08/2008	Washington DC
freedomtotinker.com	Freedom To Tinker...is your freedom to understand, discuss, repair, and modify the technological devices you own	Education/Blog (NSA)	27/09/2008	Princeton, New Jersey

ftc.gov	Federal Trade Commission	Government Agency (SA)	02/08/2008	Washington DC
gao.gov	US Government Accountability Office	Government Agency (SA)	02/08/2008	Washington DC
gilc.org	Global Internet Liberty Campaign	Advocate (NSA)	02/08/2008	Washington DC
gnu.org	GNU Operating System	Software (NSA)	11/10/2008	e-mail addresses only
gnupg.org	The GNU Privacy Guard	Software (NSA)	30/08/2008	e-mail addresses only
googleblogspot.com	Blog Site	Search Engine Blog (NSA)	27/09/2008	Google in Mountain View California
gpoaccess.gov	GPO Access: A Service of the U.S. Government Printing Office	Government Agency (SA)	30/08/2008	Washington DC
guardian.co.uk	The Guardian	News/Media (NSA)	30/08/2008	London, UK
gunowners.org	Gun Owners of America	Reference/ Interest Group (NSA)	30/08/2008	Springfield, Virginia
gwu.edu	The George Washington University	Educational (NSA)	02/08/2008	Washington DC
hasbrouck.org	The Practical Nomad	Reference Site (NSA)	08/11/2008	San Francisco
healthprivacy.org	Health Privacy Project	Advice and Advocate (NSA)	30/08/2008	Washington DC
heise.de	Heise Online	News/Media (NSA)	30/08/2008	Hannover, Germany
hhs.gov	United States Department of Health and Human Services	Government Agency (SA)	02/08/2008	Washington DC
hrw.org	Human Rights Watch	Advocate (NSA)	02/08/2008	London, UK
icann.org	Internet Corporation for Assigned Names and Numbers	Advocate (NSA)	02/08/2008	Brussels, Belgium
ico.gov.uk	Information Commissioner's Office, UK	Government Representative (SA)	30/08/2008	London, UK
ifea.net	Internet Free Expression Alliance	Advocate and Research (NSA)	02/08/2008	e-mail address only
indymedia.org	Independent Media Centre	News/Media (NSA)	02/08/2008	London, UK
intgovforum.org	The Internet Governance Forum	State Level Operative (Agency of the UN) (SA)	02/08/2008	Geneva, Switzerland
ipc.on.ca	Canadian Information Commissioner's Office	Government Representative (SA)	02/08/2008	Toronto, Ontario
iris.sgdg.org	Imagions un Réseau Internet Solidaire	French Affiliate of EDRI (see EDRI)	02/08/2008	(see EDRI)

isoc.org	Internet Society	Research (NSA)	16/08/2008	Reston, Virginia (Headquarters)
jamesmadisonproject.org	James Madison Project	Advocate (NSA)	30/08/2008	Washington DC
junkbusters.com	JunkBusters: Bust the Junk Messages Out of Your Life	Commercial/ Application (NSA)	02/08/2008	Gillette, Wyoming
justice.gov.uk	Ministry of Justice	Government Agency (SA)	11/10/2008	London, UK
latimes.com	The LA Times	News/Media (NSA)	02/08/2008	Chicago, Illinois
lessig.org	Lessig	Research (NSA)	16/08/2008	Stanford, California
libertycoalition.net	Liberty Coalition	Advocate (NSA)	16/08/2008	Washington DC
liberty-human-rights.org.uk	Liberty	Advocate (NSA)	02/08/2008	London, UK
my.barackobama.com	Barack Obama and Joe Biden: The Change We Need	Campaign Site for the American Presidential Election (SA)	02/08/2008	Chicago, Illinois
myspace.com	My Space: Social Networking Site	Social Networking Site (NSA)	02/08/2008	Herndon, Virginia
news.bbc.co.uk	BBC News	News/Media (NSA)	27/09/2008	London, UK
no2id.net	NO2ID	Advocate (NSA)	02/08/2008	London, UK
nocards.org	CASPIAN	Advocate (NSA)	02/08/2008	US
nytimes.com	New York Times	News/Media (NSA)	02/08/2008	New York, New York
oecd.org	Organisation for Economic Co-operation and Development (OECD)	State Level Operative (SA)	02/08/2008	Paris, France
pandab.org	Privacy, Business and Law	News/Media (NSA)	02/08/2008	Only contactable through online form
peacefire.org	Peacefire: Open Access for the Net Generation	Advice/ Technical (NSA)	02/08/2008	Bellevue, Washington
pgp.com	PGP Co	Commerical (NSA)	02/08/2008	Uxbridge, UK
pgpi.org	The International PGP Home Page	Software/ Resource (NSA)	02/08/2008	E-mail address only
pogo.org	Project on Government Oversight	Independent Auditor (NSA)	02/08/2008	Washington DC
privacy.org	Privacy.org	Advocate (Collaboration between PI and EPIC)	02/08/2008	See PI and EPIC (London)
privacyactivism.org	Privacy Activism	Advocate (NSA)	02/08/2008	Only e-mail address listed

privacyinternational.org	Privacy International	Advocate (NSA)	02/08/2008	Washington DC
privacyjournal.net	Privacy Journal	Advocate and News/Media (NSA)	02/08/2008	Providence, Rhode Island
privacyrights.org	Privacy.org	Advocate (NSA)	02/08/2008	San Diego, California
privacytimes.com	Privacy Times	News/Media (NSA)	02/08/2008	San Diego, California
publicknowledge.org	Public Knowledge: Fighting for your digital rights in Washington	Advocate (NSA)	13/09/2008	Washington DC
rcfp.org	The Reporters Committee for Freedom of the Press	Advocate (NSA)	02/08/2008	Arlington, Virginia
realnightmare.org	Real Nightmare (ACLU)	Advocate (NSA)	02/08/2008	New York, New York
regulations.gov	Regulations.gov: Your voice in Federal decision-making	Government Agency (SA)	02/08/2008	Only e-mail address listed
rsf.org	Reporters Without Borders	News/Media (NSA)	02/08/2008	Paris, France
schneier.com	Bruce Schneier	Research (NSA)	02/08/2008	e-mail address only
soros.org	Open Society Institute & Soros Foundations Network	Foundation (NSA)	02/08/2008	New York, New York
spamcop.net	SpamCop.net	IT Advice (NSA)	02/08/2008	US (exact location unknown[32])
spychips.com	SpyChips: Affiliate of no.cards.org (CASPIAN)	Advocate (NSA)	02/08/2008	US (exact location unknown)
statewatch.org	Statewatch	Advocate (NSA)	02/08/2008	London, UK
thomas.loc.gov	The Library of Congress: Thomas	Government Agency (SA)	02/08/2008	London, UK
tor.eff.org	Tor: anonymity online	See EFF	02/08/2008	See EFF
trac.syr.edu	Transactional Records Access Clearinghouse (TRAC)	Education (NSA)	02/08/2008	Syracuse, New York
un.org	The United Nations	State Level Operative (SA)	02/08/2008	New York, New York
unhchr.ch	Office of the Higher Commissioner for Human Rights	Government Representative (SA)	02/08/2008	New York, New York
usdoj.gov	The US Department of Justice	Government Agency (SA)	11/10/2008	Washington DC
usatoday.com	USA Today	News/Media (NSA)	02/08/2008	McLean, Virginia
wiki.vorratsdatenspeicherung.de	Ak Vorrat	Wiki and Advocate (NSA)	16/10/2008	Bielefeld, Germany

[32] This can occur for several reasons including the author having a personal address, which they do not wish to reveal online or the site only contains a form or box for mailing queries, as opposed to an e-mail, telephone or postal address.

wired.com	Wired News	News/Media (NSA)	02/08/2008	New York, New York
youtube.com	YouTube	Social networking Site (NSA)	02/08/2008	San Bruno, California