Democratic heroism - Directive 2006/24/EC and the struggle for the soul of democracy

Karlsson, Rasmus

2008

Paper presented at

2nd ECPR Graduate Conference
25-27 August 2008, Barcelona, Spain

RASMUS KARLSSON

Democratic heroism

– Directive 2006/24/EC and the struggle for the soul of democracy

LUND
UNIVERSITY

Department of
Political Science

ABSTRACT

In the debate on how to make democracy strong against terrorism, it has been suggested that the Western democracies need new protective measures. This paper argues that, far from protecting democracy, such measures may in fact undermine the very values and virtues that make democracy possible.

Information freedom, the right to due process and the protection of privacy are all fundamental for the functioning of a democratic society. Despite this, recent years have seen a string of new laws, both in the US and in Europe, that in different ways curtail key civil liberties. Even countries entirely unaffected by international terrorism, such as Sweden, have passed new legislation allowing electronic surveillance and covert listening devices. Taking the recent Swedish legislation as its starting point, the paper will also address the related EC directive on data retention (2006/24/EC). A key question posed is to what extent democracy has to be based on courage or even "heroism" if it is to remain true to itself when confronted by terrorism or other existential threats.

Key words: Political theory, Democracy, Terrorism, Electronic Surveillance

Introduction

In the two days leading up to its summer recess, the Swedish parliament became a scene of surreal drama as thousands of democratic activists, all dressed in white, gathered to protest the passing of a new electronic surveillance law[1]. Once enacted, the law would allow continuous filtering of all international telecommunications and internet traffic entering or leaving Sweden. The white colour had been chosen to symbolize innocence. If the law was to pass, the activists argued, the distinction of legal innocence would be blurred as everyone was theoretically to be subject to the government eavesdropping.

Despite massive protests, the law which pejoratively had become known as *Lex Orwell* passed late in the evening of 18 June 2008. While probably in violation of both the Swedish constitution[2] and the European Convention on Human Rights (ECHR)[3], the new law marked but a continuation of a rapid legal development circumscribing privacy rights in Sweden[4]. Undoubtedly, this legislative

---

[1] Government proposal 2006/07:63 – "*Changes to defence intelligence activities*"

[2] In the Swedish constitution, the Instrument of Government (Regeringsformen) is the first of four foundational laws and it addresses, among other things, fundamental rights and freedoms. Its second chapter provides protection against invasion of privacy and examination of confidential communications. These rights however are not absolute and can be restricted in an ordinary act of law. Such restrictions must none the less be of a kind "acceptable in a democratic society" and must not exceed what is "necessary having regard to the purpose which occasioned it". Furthermore, any restrictions must not be carried "so far as to constitute a threat to the free formation of opinion as one of the fundaments of democracy". Given the role that the internet has come to have as an arena for public debate and the dissemination of opinions and ideas, it is reasonable to argue that mass-surveillance of all international internet traffic (including everything from citizens joining Facebook-groups to what books they order at Amazon) constitutes precisely a threat against the "free formation of opinion". Unfortunately, since Sweden does not have a constitutional court (as in Germany) nor abstract juridical review (as in the United States), it is possible for Sweden to have laws which violate the rights provided in the constitution.

[3] In a case from this year, "Liberty and Others v. The United Kingdom" (application number 58243/00), the European Court of Human Rights ruled that any system of secret monitoring of communications must have minimum safeguards set out in statute law in order to avoid abuses of power. These safeguards have to include the nature of the offences which may give rise to an interception order, limits to the duration of surveillance, and a definition of the categories of people liable to surveillance. The court ruled that these safeguards apply both to measures of surveillance targeted against individuals and more generalised "strategic monitoring". Since these safeguards were lacking in the case (just as they are in the new Swedish law) the court found the United Kingdom to be in violation of the rights provided under Article 8 of the ECHR.

[4] Other new laws mandate the use of covert listening devices (Governmental proposal 2005/06:178), domestic wiretapping and the use of "surplus information" in criminal investigations (Governmental proposal 2004/05:143)

flurry fits well into a larger international trend symptomatic of the post-9/11 political landscape. At the same time, there may be reasons to treat the Swedish case with some special interest. Not only does Sweden stand out with its long history of political stability and its highly consolidated democracy. Due to its geographic location and other reasons, it is also a country which has remained practically untouched by international terrorism. With this in mind, Sweden can be seen as sort of a *crucial case*: if its government is willing to trade freedom for perceived security gains, there should be little holding back countries and governments which for one reason or the other consider themselves closer to the fray.

However, before going further into the empirical material, I would like to say something about this paper as such. From the beginning it is a normative piece, to be read more as a short opinion paper than a scientific article. It is written by a political theorist who, though he has studied informatics, normally engages with very different questions. A further disclaimer regarding the scientific ambitions of this paper stems from the fact that much of the empirical material is still rapidly changing or classified. With this in mind I have tried to formulate an argument that holds irrespectively of particular technical details even as these details may remain important for our background understanding. Finally, it is worth point out that I am aware that many claims made in the paper would require further sources prior to any publication.

Theoretically, it seems instructive to start with a simple distinction: in a democratic society, it is those who govern who are to be transparent and not those who are governed. The first to secure accountability, the second to protect political privacy. To exemplify, we expect our politicians to provide public justification for their decisions, yet we protect the secrecy of the ballot box. Public hearings, parliamentary debates and different national "freedom of information acts" are there to facilitate responsibility towards the electorate. At the same time, we are instinctively repelled when we find out that the state for instance has registered people on basis of their political views, religious faith or sexual orientation. The importance of privacy is simply fundamental and poll data suggest that, over the last fifteen years, around 80 percent of all Americans have consistently considered it to be "essential"[5].

[5] Best, Samuel, Krueger, Brian and Ladewig, Jefrey (2006) *Privacy in the Information Age*, page 376

It can be argued that it is this fundamental distinction which traffic analysis, blanket data retention and the kind of "information trawling" authorized by the new Swedish law have come to undermine if not invert. The geographical pinpointing of cell phones, the possibility to use data-mining to search for unusual patterns in personal communication and the ever more widespread use of closed-circuit television all allow those who govern to monitor the governed, often in ways so intrusive that they would have been politically unthinkable only a few decades ago. Once the data has been gathered, the individual citizen has little if any control over how it is used. From a democratic theoretical point of view, the importance of this shift does not lie in its practical applications (if the state will indeed misuse its new authorities) but rather how democracy itself is eroded in a society where everyone knows that they are potentially subject to government surveillance.

On the basis of this distinction of transparency, the main aim of the paper will be to explore the idea of "democratic heroism" as a possible alternative to the prevailing security-oriented paradigm.

Frontlines of democracy

In a time when ever more social interaction is taking place via telecommunications networks, it is not surprising to find that the frontlines of democracy are also becoming increasingly digitalized. New technologies are opening up formerly unanticipated potential for surveillance just as the fear of terror are driving many countries in an illiberal direction. Though Guantanamo and Abu Ghraib may be the exceptions, the last years have seen key liberties frayed both in the United States and in Europe. Ranging from extensions to the maximum time a suspected criminal can be held without charge to the murky practice of secret renditions, the bending of legal language has allowed for a whole set of new measures aimed at "protecting democracy". Unsurprisingly, many have argued that these measures have had the opposite effect, eroding the sense of "who we are" and giving in to precisely the kind of fear which the terrorists want to project.[6]

In the realm of information technology, the focus on national security and the corresponding anti-terrorism measures have, in particular, been played out along two emerging "frontlines":

[6] Barber, Benjamin (2003) *Fear's Empire: War, Terrorism, and Democracy*

- The introduction of mass-surveillance systems based on advanced filtering techniques and computerized trawling
- The passing of new laws mandating blanket data retention of traffic data

On the first frontline, the situation differs significantly from country to country. While the United States traditionally has been the "leader" with the massively funded National Security Agency (NSA) and the sweeping authorities provided through the USA Patriot Act of 2001, the governments of other democracies such as Britain and Sweden have been eager to move in the same direction.

While signals intelligence services historically have been monitoring air-based transmissions (and then primarily military radio traffic), the focus is now clearly on non-military cable-based communications. In the Swedish case, the new law mandates that, effective 1 October 2009, all telecommunication service providers will have to physically route their traffic through a number of "co-operation hubs" at which the National Defence Radio Establishment (FRA) will be able to extract an exact copy of all international traffic as it crosses the border. The FRA will then scan these data streams on basis of a large number of "technical parameters", discarding all data which does not fit a predefined search profile. In the heated debate, this procedure has caused a lot of confusion. Proponents of the new law, including the director of the FRA Ingvar Åkesson, have argued that the law does not amount to mass-surveillance since the FRA will not be able to store or analyze more than a fraction of the data gathered through the system.[7] However, as many rightfully have pointed out, if there is a rights violation, it happens already when the FRA breaks the communications confidentiality and apply their search filters.

Unlike more targeted surveillance schemes in other countries, the FRA will not be required to obtain a court order to undertake surveillance of citizens' communications. Though there are some limits to their mandate (basically that all searches should concern "external conditions") there is nothing preventing the FRA from gathering information about particular individuals by studying what international websites they visit, listening to what they say on the phone when calling abroad or creating complete sociograms mapping out personal networks.

[7] Svenska Dagbladet (2008-06-29) *FRA kan inte spana på folket*, page 5

Traditionally in democracies, such far-reaching authorities have been given only to the police when pursuing a particular criminal investigation. Similarly, wiretapping of phones used to require a court order and were always limited in duration. However, as national signals intelligence agencies are increasingly orienting themselves against so called "new threats", many of these established principles seem to be in fluctuation. As I will argue on a more general level later, I hold both mass-surveillance and blanket data retention to be most detrimental to the flourishing of democracy. Furthermore, there is a range of more specific democratic problems which come with electronic mass-surveillance as such. In many countries, communications with journalists, doctors, and lawyers enjoy special legal protection. In Sweden, anyone is allowed to anonymously give material to the media and the state is also prevented from further investigating the source (unless there has been a clearly defined breach of secrecy which for instance compromises national security). With the new surveillance law, it is possible that communication originating from for instance Hotmail or other international e-mail providers will be intercepted on their way to Swedish newspapers or other media. In such cases the FRA has promised to immediately delete the acquired information. Reassuring as that may sound we have to keep in mind that it may require legal expertise to determine if the recipient is indeed a journalist. If confronted with highly sensitive political information, there is an obvious risk for leakages as the number of people involved grows. It seems safe to conclude that the more information that the state and its agencies are allowed to gather in the first place, the more pronounced such risks will be.

Turning to the second frontline, the situation is somewhat more homogenous with the European Union having adopted a common directive in March 2006. The directive, EC 2006/24/EC, mandates that communications providers must retain, for a period of between 6 months and 2 years, data that allows authorities to trace and identify:

- The source of a communication
- The destination of a communication
- The date, time and duration of a communication
- The type of communication device
- The location of mobile communications equipment

The directive as adopted covers fixed telephony, mobile telephony, internet access, internet e-mail and internet telephony. When debated in the European Parliament, the Civil Liberties, Justice and Home

Affairs committee had recommended data to only be retained for a maximum of 12 months and only to be made available for crimes serious enough to qualify for a European arrest warrant. However, these recommendations, as well as the need for an explicit juridical warrant, were put aside.

Practically, the directive stipulates that every time someone makes a phone call, sends or receive an sms or an e-mail, the service provider in question must retain a record of the communication.[8] In the case of mobile devices, the geographical position is also to be stored, enabling the plotting of detailed maps showing the movement patterns of particular individuals.[9] Considering how integrated for instance cell phones have become in our daily lives, these records are likely to contain highly sensitive personal information (including everything from love affairs to for instance contact with help-lines for substance abuse etc).[10] Politically, cell phones and then in particular text messages, have been instrumental in organizing democratic protests, as seen in demonstrations everywhere from South Korea to Manila.[11] It is with this in mind that we should recognize that blanket data retention "constitutes a permanent, general recording of citizens' behaviour"[12].

Before the EU-directive was issued, communication service providers were often legally prevented from retaining data beyond what was necessary for billing purposes. In some cases, providers, claiming the right to confidentiality of their customers, were hesitant to co-operate with government authorities. Now the directive mandates retention for a minimum of six months (and individual member states may even mandate retention beyond the maximum two years stipulated in the directive) and that the retained data is made available to "competent national authorities" as defined by each member state.

---

[8] Though I will not pursue that argument further here, one may argue that data retention cannot prevent acts of terror but merely assist the police in finding the culprits once an attack has taken place. Similarly, it can be argued that terrorists can easily avoid detection by using anonymous pre-paid SIM-cards, stolen phones or web-based e-mail services.

[9] Bowden, Caspar (2002) *Closed Circuit Television for Inside Your Head: Blanket Traffic Data Retention and the Emergency Anti-Terrorism Legislation*

[10] It is worth pondering that if people know that data retention is in place it becomes not only a question of what to do or not but also a question of how things can be interpreted. To give a crude illustration we can think of a middle-aged male politician whose elderly mother happens to live in a house along one of the main prostitution lines in the city. Every Friday night he comes home to her for dinner. In a world of data retention that behaviour is immediately seen as highly suspect.

[11] Rheingold, Howard (2002) *Smart Mobs: The Next Social Revolution*

[12] Breyer, Patrick (2005) *Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR*, page 370

"Freiheit statt Angst"

If these now are the frontlines, it is interesting to ask who is fighting at what side. Compared to the old days of the Cold War it appears far more difficult to draw a simple picture. Though human rights were certainly infringed also in the West from time to time, the basic struggle between the open liberal democracies of the West and the closed authoritarian regimes of the East was there for everyone to see. This bipolarity provided an immediate mirror; just think of how surprised the Russians, who were certain that democracy was but a façade, were when Richard Nixon had to resign for his involvement in the illegal wiretapping during the Watergate scandal. Today, without that mirror, the fight for the open society may in itself seem to be but a relic from another time. In its most extremes we hear that "9/11 changed everything". Luckily, there are still many of us who think it did not.[13] Yet, to argue in favour of civil liberties and against further surveillance measures means to confront a Zeitgeist which seems to become ever more obsessed with "security". I believe that what is most of all missing is an alternative (positive) vision, a vision which illustrates the importance of remaining true to our democratic ideals and practices even, or maybe especially, in times of fear.

One way to continue this article would be to challenge the empirical judgement which says that we have reason to feel that fear in the first place. That however, would take us deep into the realm of international relations and, to a certain extent, into idealistic speculation about the future. Though I am always tempted to go down that road, I am not going to do it this time. Instead I will argue that what we need in times of fear, be it well-founded or not, is courage.

Let me begin with an example which probably already has figured in a textbook or two. Every year around 600 people die in traffic accidences in Sweden. If Sweden was to impose a general speed limit of 30 kilometres an hour, a large number of these deaths would be

[13] In a memorable judgement from 2004, the British law lord Leonard Hoffman brought much needed perspective to the threat of terrorism: "this is a nation [Britain] which has been tested in adversity, which has survived physical destruction and catastrophic loss of life. I do not underestimate the ability of fanatical groups of terrorists to kill and destroy, but they do not threaten the life of the nation. Whether we would survive Hitler hung in the balance, but there is no doubt that we shall survive Al-Qaeda." Further, talking on the special detention orders issued following the 9/11 attacks: "the real threat to the life of the nation, in the sense of a people living in accordance with its traditional laws and political values, comes not from terrorism but from laws such as these. That is the true measure of what terrorism may achieve."

prevented. Still no one would suggest such a thing. There are simply other values, be it economic growth, access to the countryside or popular opinion, which trump our will to save lives. In effect, this means that the politicians of Sweden every year "sacrifice" the life of hundreds to gain those other valuable things. Nothing strange so far. But let us now consider the case of terrorism. So far, no one in Sweden has been killed or even injured due to terrorism over the last three decades.[14] Still, it is precisely the fear of terror which is used to motivate infringements of privacy rights. With reference to the Madrid and London bombings of 2004 and 2005 respectively, it is argued that Swedes have to accept considerable loss of privacy in the name of "security". What is completely missing from this line of reasoning is the understanding that democracy does not come for free, that the open society may require courage and, ultimately, sacrifice on behalf of its citizens.

Thinking of the terrible suffering that for instance the population of London had to endure during the Second World War in the name of freedom and democracy, that thought does by no means stand out as controversial from a historic perspective. Yet, it would be obvious political suicide to try to argue along such lines in any of those morning television sofas, especially in the unlikely event of an actual terror attack. As an academic however, one is hopefully somewhat more free to think about proportionality.

Accepting that the open society may require sacrifice does not mean that it passively should await terror to strike. It only means that if it is to fight its enemies, it is to do so by the means available to democracies: by respecting the right to privacy, by protecting citizens and aliens alike from arbitrary arrest and detention, and maintaining a clear focus on the long-term aim of advancing freedom.

This may sound bombastic but it points towards the price of not honouring those principles. It is a fundamental choice, either the Western democracies continue to slide in an ever more repressive direction[15], emphasizing state control at the price of social trust. Or they commit themselves to the virtues of "democratic heroism" and

[14] The staple response to this would of course be that Sweden has been safe precisely because of the surveillance carried out by its intelligence agencies during this period. But if we accept that argument it is tempting to ask why we need all these new laws if our counter-terrorism activities already have proven so successful in the past?

[15] Characteristic of this departure from civil society is the lack of accountability and proportionality which comes with the declaration of different "wars", such as the "war on terror" or the "war on drugs"; Walker, Clive and Akdeniz, Yaman (2003) *Anti-terrorism Laws and Data Retention: War is over?*, page 182

begin moving in the opposite direction. Since democracy ultimately can be seen as being about information exchange[16] it is not difficult to understand why both electronic mass-surveillance and data retention go to the heart of this choice.

References

Barber, Benjamin (2003) *Fear's Empire: War, Terrorism, and Democracy*, New York: W.W. Norton & Co

Best, Samuel, Krueger, Brian and Ladewig, Jeffrey (2006) *Privacy in the Information Age*, Public Opinion Quarterly, 70(3), 375-401

Breyer, Patrick (2005) *Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR*, European Law Journal, 11(3), 365–375

Bowden, Caspar (2002) *Closed Circuit Television for Inside Your Head: Blanket Traffic Data Retention and the Emergency Anti-Terrorism Legislation*, Computer and Telecommunications Law Review, March 2002

Rheingold, Howard (2002) *Smart Mobs: The Next Social Revolution*, Cambridge, M.A.: Perseus Publications

Sundström, Mikael (2001) *Connecting Social Science and Information Technology – Democratic Privacy in the Information Age*, Lund: Lund University

Svenska Dagbladet (2008-06-29) *FRA kan inte spana på folket*

Walker, Clive and Akdeniz, Yaman (2003) *Anti-terrorism Laws and Data Retention: War is over?*, Northern-Ireland Legal Quarterly, 54(2), 159-182

* * *

Biographical note:

Rasmus Karlsson is a PhD Candidate in political science at Lund University, Sweden. His research interests traverse theories of intergenerational justice, sustainable development, and the temporal dimension of democracy. In fall 2008 he will be a visiting scholar at the University of Melbourne, Australia.

The author can be contacted via e-mail rasmus.karlsson@svet.lu.se. More on the debate about *Lex Orwell* and the data retention directive can be found on his weblog at www.rawlsandme.blogspot.com.

[16] Sundström, Mikael (2002), page 114