Transnational e-government systems: A tale of European integration and surveillance

Georgia Foteinou
University of Patras, Greece
gfoteinou@upatras.gr

Abstract

The EU decision to deploy a “Data compilation instrument”[1] to spy on radicals has triggered a contentious academic and political debate on the limits of “home security”, privacy and state surveillance. The plan that constitutes part of the European counter-terrorism strategy will permit states to monitor citizens’ activity and beliefs in order to unveil and classify “radicals”. Anyone who may be classified as anti-globalisation, islamist, extreme right or left, nationalist etc. will become subject to extensive monitoring and surveillance. The proposed data compilation instrument will permit sharing and compilation of detail personal data (economic situation, psychological traits, type of education, work experience etc.) from various sources in order to define the ideology and political beliefs of EUs citizens that are labelled as “radicals”. What new this instrument brings to EU security policies is that is targeting "radicalisation" instead of terrorism. However, being radical does not imply being terrorist and there is a question on how democratic societies can operate without dissidents.

This emerging security-informational complex which will be based on intergovernmental IT systems that facilitate surveillance and monitoring of “radicals” puts in question the totalitarian tendencies of democratic liberal states through ICT. Can such policies move Europe towards a total surveillance state or there are ways of making it compatible with civil liberties and democratic principles? The main issues to be analysed in this paper is the 'europeanization' of surveillance and the classification and labelling of citizens as a means of social control and discrimination.

1. Introduction

The advent of computer technology in all aspects of governance and government – the so-called eGovernment technology – has brought to the fore not only issues of productivity and automation but also a whole new universe of monitoring and surveillance capabilities. Monitoring and controlling all aspects of social and political life is now becoming cheaper and faster than ever before. Technology enables governments across Europe to monitor virtually every aspect of citizens' life. How much they spend, what do they believe, where do they travel, where do they live, what is their age, job, preferences, special circumstances etc. are only a few of the questions that can be answered with the use of the right data gathering systems. Every phone call made, every text message and email sent and each website accessed, will be – and it already is in some countries – subject to monitoring and surveillance by government agencies.

Recently, the Council of the European Union announced the introduction of a "Data compilation instrument" to spy on groups of radicals. The implementation of such technological instrument has triggered a contentious academic and political debate on the limits of "home security", privacy and state surveillance. The plan that constitutes part of the European "war on terror" will permit states to monitor citizens' activity and political ideology in order to unveil sources of "radicalisation". The tricky issue here is, first and foremost, "what a radical is?" According to the EU a "radical" is anyone who may be labelled as islamist, anti-globalisation, extreme right or left, nationalist etc. These groups of citizens will become subject to extensive monitoring and surveillance by the EU or the EU member-states. In other words, the Council of the European Union – a supranational official body - has decided that it is important to define and classify the ideology of European citizens, even if it is certain that the great majority of them does not constitute any real threat to social peace.

In more detail, the recommended data compilation instrument will permit gathering and compilation of detail personal data (economic situation, psychological traits, type of education, work experience etc.) from various sources in order to define the ideology and political beliefs of certain groups of EU citizens.[1] What new this instrument will bring to EU security policies is that is targeting "radicalisation" instead of terrorism. However, being "radical" does not imply being a threat to social order or being terrorist. The issue of how and who defines what a radical is, raises questions that go beyond the usual debate on counter-terrorism policies. Also, the classification and sorting of citizens according to their political beliefs can be considered a form of social discrimination that may lead in actual consequences in their lives.

Governments across Europe are gathering private data to be used by public agencies for future – unspecified - purposes.[2] Citizens, courts and human rights groups have already declared this arrangement unconstitutional in a number of countries such as Germany, Romania and the Czech Republic, while in other countries these plans have simply passed unnoticed. In the UK the Communications Data Bill, which confirms the proposal to monitor in real time every communication in the country, was included in the Queen's speech to open the 2012 new session of Parliament.

[1] COUNCIL OF THE EUROPEAN UNION, 30/3/2010, Document 5692/1/10 REV 1 ADD 1 REV 1 ENFOPOL 24 'Instrument for compiling data and information on violent radicalisation processes', Brussels.

[2] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC;

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

De Vries K. Belladona R. De Hert P. & Gutwirth S. (2010), 'The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't it?)', in GUTWIRTH S. et al. (eds), Data Protection: An Element of Choice, Springer, Dordrecht

However, these plans and the arguments about "home security" can hardly sustain validity after consideration of the threat European democracy faces by such policies. By definition, the fact that it is possible for a government to monitor the data of innocent people who are not suspected of any crime means that the EU blatantly contravenes the privacy principles provided by article 8 of the European Convention on Human Rights. Also the fact that anti-globalisation is classified as "radicalism" is totally ungrounded as globalisation is viewed by the great majority of Europeans with antipathy.[3] Because, in the eyes of Europeans, globalisation is held responsible for the high levels of unemployment, the stagnant wages, the widening inequality and the destruction of the welfare state.

2. A Safer but Less Free Europe: Is There Really a Trade-Off?

Before explaining in detail what the European legislation and policies are, it is important to present the two sides of the debate. It is also important to see the broader picture as surveillance has come to be seen as a phenomenon of major importance in modern societies. Surveillance is questioning the boundaries of public space, social justice and the parameters of state power, and calls for re-thinking of the European social contract. Typically, social contract theories imply that individuals agree to surrender some of their freedoms to the government in return for protection of their rights. The legitimacy of the state's power over individual freedoms is thus challenged through surveillance because fundamental rights – such as the right to openly disagree with state policies and the right to privacy – are violated.[4]

We also need to take into account the crime control and risk assessment techniques. Because, there is ideological and normative power in European directives and recommendations which needs to be taken into account, while the false demarcation between the technical and normative aspects of state control may dictate what is "politically correct" just by using the right "instrument".[5] Because it is true that sometimes the means is the message and the instrument has more normative power than the idea itself. Nevertheless, the EU is going ahead with privacy intrusive policies even if they recognise there are serious flaws in their plans. Last year, the EU Home Affairs Commissioner Cecilia Malmstrom defended the controversial data retention law explaining that it is "necessary" and thus it will not be scrapped, despite data privacy issues and constitutional court rebuttals in several member states. "Data retention has proven useful in criminal investigations, but there is need for improvement as regards the design of the directive so that it better respects both the security and the privacy of our citizens," Cecilia Malmstrom pointed out during a press conference.[6]

Therefore, on one side of the debate, there are the advocates of surveillance as part of the "counter-terrorism" policy. Their argument is that the government owes to provide a safe and peaceful environment to its citizens, and therefore monitoring and surveillance is part of the "crime prevention" strategy while the citizens' classification is part of the *risk assessment*. The government through surveillance tries to tackle terrorism, tax evasion, bank fraud etc. and the citizens need to accept the violation of their privacy for that purpose. Their justification is that surveillance is necessary even at the expense of civil rights violations.

However, we should not forget that in democracy the legitimacy of such bold directives lays on the

[3] 'Greece tops list of anti-globalization countries, survey shows', available on http://english.peopledaily.com.cn/200506/07/eng20050607_188851.html The world-wide survey was conducted by TNS-ICAP in cooperation with the Gallup International Association in 64 countries spread over five continents. It shows that a 56 percent majority of world citizens are opposed to globalization, believing that it creates more problems than it solves. Greece topped the list, with 72 percent of the respondents in agreement with that opinion.

[4] Coleman R. (2003), "Images From a Neoliberal City: The State, Surveillance And Social Control", *Critical Criminology*, issue 12, p. 21-42

[5] Coleman (2003), p. 22

[6] Pop V. (2011), 'EU commission defends telecoms surveillance law', *EU Observer*

citizens perceptions of what is acceptable and what is not. The legitimacy of a law or a directive lays on the ethics of a given society, it is not universal and it cannot be implemented in any country regardless of the cultural background. The "one that fits all" simply doesn't apply. Under current provisions of the data retention law, internet and mobile phone providers are required to retain detailed data of calls and emails for a period between between six months to two years, while police and intelligence services are able to track and analyse calls and emails for the purpose of crime investigation. However in practice, as the European Commission admits in its report, the access on data retention varies significantly across member states. For example, the data retention law is not being applied in Germany, Sweden, Austria, Romania and the Czech Republic as it was blocked either by the respective constitutional courts or the parliament. In contrast, in Poland data is stored for the longest period and although the police mostly handle data inquiries to telecom providers, the country's national legislation does not clearly specify that it should be used only for serious offences, leaving space for spying on many other citizens groups.[7]

Under theses circumstances, there are many official bodies, NGOs and analysts who voice an open warning over these laws implementation in the EU. European Digital Rights (EDRi), a transnational organisation for digital civil rights, performed a detailed assessment of the data retention law and concluded that EU citizens are experiencing an unprecedented invasion in their privacy and that *they gained nothing out of this law.*

"*In 2010, the average European had their traffic and location data logged in a telecommunications database once every six minutes*" EDRi points out. At the same time the European Data Protection Supervisor states that data retention is "*the most privacy-invasive instrument ever adopted by the European Union*" while NGOs and interest groups express their concerns over privacy violation in several occasions. Therefore, nothing can guarantee privacy protection in the EU as every citizen is viewed as potential criminal. Because the "instrument" or the "directive" is used to define what is politically acceptable in the public and private space alike as any IT instrument has embedded in its code rules, values and morals.[8] It is, in other words, the technical implementation of a political idea.

For example, the "Data Compilation Instrument" implies that the discussion of anti-globalisation ideas is not allowed. And the immediate question is who decided that for our societies and why. How an unproven economic theory, this of unconstrained deregulated international markets, becomes a "politically correct" idea while the opposite becomes "persecuted"? Is it illegal to talk openly or even to demonstrate against market failures and the disasters of these economic dogmas? Maybe this is what Joseph Stiglitz, the famous Nobel laureate in economics, means when he says that this economic crisis is a "doctrine made" crisis.[9] Because policy makers are following some kind of economic dogma rather than a rational economic policy.

The key question here, is do we have to sacrifice our privacy in order to secure social peace? Does this mean that when one is reduced, the other is automatically increased? We need here to take a step back and see the whole picture. Aristotle was arguing that "poverty is the parent of revolution and crime" and it is indeed true that societies with higher inequalities – especially economic inequality – are more prone to crime than egalitarian societies. Therefore, unless we see the causes of radicalism we cannot prevent people from becoming radicals just by spying on them. This is more a form of suppression rather than a form of prevention.

Daniel Moecli (2008) argues that unless someone holds an over simplistic and overly abstract

[7] Pop V. (2011), 'EU commission defends telecoms surveillance law', EU Observer

[8] D. Lyon (2003), 'Surveillance as social sorting: Privacy, Risk and Digital Discrimination', Routledge, New York, p. 20

[9] J-P. Fitoussi, J. Stiglitz (2009), Document de Travail: "« The Ways Out of the Crisis and the Building of a More Cohesive World » N° 2009-17 Juillet 2009"

conception of liberty and security this trade off between freedoms and security does not stand.[10] There is no evidence that more surveillance leads in safer societies. In fact, those countries that suffer the most from radicalism and terrorists attacks are the ones who have their citizens under close scrutiny – namely the US and UK. There is no indication that these countries have lower crime rates now than before the introduction of such instruments. Therefore, it seems that there is not exactly a trade off between freedoms and home security, but between freedoms and surveillance. Because there are of course other ways of protecting social peace without violating privacy rights and the EU states need to find and implement them.

3. Radicals, obedience and political dissenters

> *"Following the resurgence of terrorist activities across the world in recent years, in 2005 the European Union developed a global counter-terrorism strategy which had prevention as one of the four strands of its strategic commitment. The purpose of that strand is to prevent individuals from turning into terrorists by tackling the factors and profound causes which may lead to radicalisation and recruitment both in Europe and elsewhere.*
>
> *In 2005 the European Union agreed on a Strategy and an overall Action Plan for Combating Radicalisation and Recruitment to Terrorism as an addition to the global counter-terrorism strategy referred to above, prompting the Member States to present various initiatives."*
> *(Council of the European Union, Brussels 16/04/2010)*[11]

What this document unveils is that in fact the EU has a "global counter-terrorism strategy". However, it is unclear to the average European what this global strategy is – and since it is global and not European – who the other actors are. With who other players the EU is coordinating its strategies and how our personal data are shared? In which databases and which agents? Also, what "terrorism" prevention means and how the EU may "prevent people from becoming terrorists"? Does this mean that we may all be constantly monitored just in case we may decide to become terrorists? What are the boundaries of this strategy? Since the percentage of terrorism victims are only a negligible number every year in Europe – at least compared to other causes, let's say the road accidents or robberies – why so radical policies are needed? Because targeting innocent people is probably a step too far in counter-terrorism policies and if this logic applies to more areas, let's say, the theft, robberies, fraud etc, then the average European may end up soon being monitored 24 hours a day for a whole range of reasons.

Since there is neither academic or legal consensus on what terrorism is, the fight on terror may become a quite tricky issue as it depends on the interpretation of the term in various directives and instruments. By checking the definition on a dictionary we see that "terrorism is the use of violence and threats to intimidate or coerce, especially for political purposes". So, when the government uses its power to intimidate citizens and to force them to change their political ideology is this an act of terrorism or not? What is the cost of counter-terrorism policies for our democracies?

We only need to remind here the Indefinite Detention initiatives in the US where the idea is to indefinitely detain people who are not terrorists but who might be proven terrorists. Thus, people

[10] D. Moecli (2008), 'Human Rights and Non-discrimination in the 'War on Terror' Oxford University Press, New York, p.26

[11] COUNCIL OF THE EUROPEAN UNION, 30/3/2010, Document 5692/1/10 REV 1 ADD 1 REV 1 ENFOPOL 24 'Instrument for compiling data and information on violent radicalisation processes', Brussels. Underlined by the author.

who did not have a trial yet but they are still in detention for an unspecified period of time.[12] Quantanamo is a notorious indefinite detention prison. Another example is the United Kingdom's Anti-terrorism, Crime and Security Act 20019 (ATCSA) that was proven extremely controversial. Dana L. Keith (2003) states: "*Its provisions stand out as radical in the degree in which they sacrifice freedom in the name of national security. More specifically, paragraphs, §§ 411 and 412 of the Patriot Act and Part 4 of ATCSA, provide the governments of the United States and United Kingdom with extensive powers to take into custody and detain non-citizens suspected of terrorism.*"[13] How far away is this from becoming a European routine? How far the EU can proceed in the name of EU security?

The whole picture looks gloomy. The Council's "data compilation instrument" might not only violate privacy rights of thousands of maybe millions of innocent people but also it might lead in actual consequences in their lives. When a citizen is labelled as "radical" or "potential terrorist" then this is an act of discrimination and it might lead in nasty consequences in their lives. The proposed data compilation instrument classifies people according to their citizenship status, their country of origin, their ethnicity, race, occupation and religion. The Council instrument is clear on that: "*Territorial, political, economic, social, historical, cultural, religious, ideological, ethnic, linguistic and social identity aspects, etc.*" should be subject to surveillance.[14]

Therefore, the issue goes beyond the usual aspects of privacy limitations and lies at the fact that the 'instrument' or the technology used is discriminatory. It obtains personal and group data in order to classify individuals and populations according to the aforementioned criteria, to determine who should be targeted for suspicion, eligibility, special treatment etc. This indicates more an attempt to manage populations as a need resulting from the destruction of the welfare state, rather than a need to combat terrorism. Because the decline of the welfare state that occurs systematically in all advanced countries has the effect of individualising the risks and citizens tend to be reactive to this. For those under risk resulting from the dismantling of the welfare state, extensive surveillance is used as means of discipline, rather than as a means of radicalism prevention.[15]

We should not forget that systems are sociotechnical. Their classification algorithms and architecture implement a very accurate idea of who should be targeted and why. As Bowker and Star state, "*values, opinions, and rhetoric are frozen into codes [...] Software is frozen organisation and policy discourse*"[16] Because, social sorting through these researchable databases means that people classified under a certain category may undergo unfair treatment because of other people classified within the same group who exhibit deviant behaviour, while at the same time they all ignore they are grouped under a specific category. Thus, what one does has impact to the others but they are all ignorant of this fact, and therefore unable to control it. The results may range from simple privacy violations to executive detention of foreign terrorist suspects (or "radicals"), selective enforcement of immigration laws and selective use of police powers.[17]

4. Why an "Instrument" and not a law: the results of its implementation

It is important to stress here that the "Instrument" proposed by the Council it is agreed in the form

[12] D. Keith (2003) 'In the Name of National Security or Insecurity?: The Potential Indefinite Detention of Non-Citizen Certified Terrorists in the United States and the United Kingdom in the Aftermath of September 11, 2001', Berkeley Electronic Press

[13] Keith D. (2003)

[14] COUNCIL OF THE EUROPEAN UNION, 30/3/2010, Document 5692/1/10 REV 1 ADD 1 REV 1 ENFOPOL 24 'Instrument for compiling data and information on violent radicalisation processes', Brussels.

[15] Lyon D., 'Surveillance as social sorting: privacy, risk, and digital discrimination', Routledge, New York, 2003, p.20

[16] Bowker J. & Star L. ()

[17] D. Moecli (2008), 'Human Rights and Non-discrimination in the 'War on Terror' Oxford University Press, New York, p.26

of policy recommendations and it is described in the Council's conclusions. This form of policy-making is known to the scholars of European Union politics as “soft law” and it might take the form of policy harmonisation before the actual introduction of EU law or when the national parliaments will definitely block a law. Because it is known that the European parliament and the national parliaments alike are much more careful and they put any proposed privacy limitations under close scrutiny.

Nevertheless, recommendations on the basis of European cooperation on security issues are legitimate and widely used in various areas. These recommendations are not only implemented but are also not subject to approval by a legislative body in any European parliament. Therefore, it does not really matter if it is law or not, since it will be finally implemented, the EU citizens will never find out the details of it (since surveillance is by definition hidden from the public) and European police forces will be instructed to perform this classification.

In fact, the problem lies exactly on this: on what Europol and national police forces will be asked to do. Because this instrument is the practical expression of a counter-terrorism strategy that allows for various interpretations and misconceptions. First, because the target is unclear. Should they target terrorists, violent radicals or just “radicals”? Since, those who fall under the first two categories are already targeted by criminal law and procedures, then, what is left to be targeted is the “radicals”.

The instrument as described in the Council document indicates that its goal is the ‘description of ideology directly supporting violence’, but which ideology is this? The answer is provided on the decision’s explanatory footnotes, it is the “*Extreme right/left, Islamist, nationalist, anti-globalisation etc.”*. Therefore a broad range of ideologies, poorly defined in the document. Who is the “anti-globalisation” radical? How will the intelligence agencies and the police across Europe define the “anti-globalisation”? What kind of data their systems will gather and analyse and in what ways? Because Europol for example is asked to “*generate lists of those involved in radicalising/recruiting or transmitting radicalising messages and to take appropriate steps*”. But whom are they going to target if by definition half of the European population opposes globalisation?

But Europol is not the only authority using this instrument. The Council's document refers to security and intelligence agencies, European police forces and other EU institutions and agencies.[18] In other words, we are talking about an instrument which implements an unspecified “global strategy”, is targeting a broad range of people, it runs on unknown systems – national and supranational – and it involves also unspecified institutions and agencies. The boundaries between public and private space are getting blurred. If I exchange emails with a friend is this subject to police scrutiny or not? And if it is, in what occasions? In other words, when our private discussions become subject of investigation? Can we still argue against globalisation with our friends or this is not a private discussion any more? Are we allowed to talk about leftist ideas or this automatically places us on the “radicals” list? These are questions that all Europeans as potential subjects of this instrument need to know. They need to know what subjects remain a private issue and what becomes a public issue.

A second issue is how are the authorities going to compile and analyse the information gathered? Because, the Council's document states that the aim is to share information across agencies and increase the quantity of data “*obtained by other, non-specific means or instruments*” (does this suggest by any means?). Yet, it is clearly stated that the information obtained will lead in assessments and “*tactical operational and/or strategic decision-making*”. So, the information

[18] StateWatch Report (2011), 'Intensive surveillance of “violent radicalisation” extended to embrace suspected “radicals” from across the political spectrum', available on Guardian.co.uk

gathered will lead in real consequences in policy-making and people's lives.

5. In Conclusion

The proposed instrument is not a law although it has actual consequences in EU privacy policies. So, apart from the problem that the whole strategy lacks democratic oversight and legitimacy, there are a number of other issues coming to the fore. First, it is that its targets are very vague. The instrument instead of narrowing down and specifying the potential threats to social peace it may end up targeting any citizen with political thought different than this of the establishment. Because under certain circumstances, any citizen may be labelled as “nationalist”, “extreme left”, “extreme right”, “anti-globalisation”, “islamist” etc. For example, at least 70% of the Greeks are now expressing their antipathy for globalisation, does this makes them “radicals”? Second, it is extremely unclear who is going to implement this instrument, on what systems, using what criteria in their algorithms and who they are going to share the data with.

British Liberal MEP Sarah Ludford has summarised the problem:

> "T*his kind of soft law doesn't really work. If they really wanted to do something serious, they would have to come up with a legal EU instrument and table it for co-decision in the European Parliament [...] The fundamental flaw of the mechanism is that by talking about "radicalisation" instead of terrorism, it includes in the same sweep swathes of political activists and dissenters*". [...] *A democratic society wouldn't work without dissenters. We didn't dismantle Communism and Fascism to start being suspicious at people who hold different views from the establishment."* [19]

Because, what finally this instrument targets might be any person who is holding ideologies different than this of the political elite or the government. Only the fact that the instrument targets political ideologies is alarming. A pre-emptive instrument suggesting taking action against potential terrorists based on, at best, mere suspicion is a step too far.[20] At the end of the day we need to pose the question: are we heading towards a post-democratic, supranational regime in Europe? Can we still talk about civil liberties in the post 9/11 era? Because the freedom to express political ideas – either in public or privately – is unquestionably the cornerstone of our democracies.

[19] Pop V. (2010), 'EU instrument for spying on 'radicals' causes outrage', EU Observer, available on http://euobserver.com

[20] Murphy C. (2011)‘EU Counter-Terrorism & the Rule of Law in a post-‘War on Terror’ World’, RSCAS Policy Paper 2011/03, Published in Scheinin M. (ed) European and United States Counter-Terrorism Policies, the Rule of Law and Human Rights

References and sources

Bigo D., Carrera S., Guild E. & Walker R. (2007), 'The Changing Landscape of European Liberty and Security: Mid-Term Report on the Results of the CHALLENGE Project'.

Bowker J. & Star L. (2008), Bowker, J. and Star , L. (1999) Sorting Things Out: Classification and its Consequences, Cambridge, MA: MIT Press

COUNCIL OF THE EUROPEAN UNION, 30/3/2010, Document 5692/1/10 REV 1 ADD 1 REV 1 ENFOPOL 24 'Instrument for compiling data and information on violent radicalisation processes', Brussels.

D. Keith (2003) 'In the Name of National Security or Insecurity?: The Potential Indefinite Detention of Non-Citizen Certified Terrorists in the United States and the United Kingdom in the ftermath of September 11, 2001', Berkeley Electronic Press

D. Moecli (2008), Human Rights and Non-discrimination in the 'War on Terror, Oxford University Press, New York

DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

Green Cowles M., Risse-Kappen T. & Caporaso J., 'Transforming Europe: Europeanization and Domestic Change', Cornell University Press, New York, 2001.

J-P. Fitoussi, J. Stiglitz (2009), Document de Travail: "The Ways Out of the Crisis and the Building of a More Cohesive World" N° 2009-17 Juillet 2009"

Lyon D., 'Surveillance as social sorting: privacy, risk, and digital discrimination', Routledge, New York, 2003

Lyon D., 'Theorizing surveillance: the panopticon and beyond', Willan Publishing, Devon, UK, 2006.

Murphy C. (2011)'EU Counter-Terrorism & the Rule of Law in a post-'War on Terror' World', RSCAS Policy Paper 2011/03, Published in Scheinin M. (ed) European and United States Counter-Terrorism Policies, the Rule of Law and Human Rights

Pop V. (2010), 'EU instrument for spying on 'radicals' causes outrage', EU Observer, available on http://euobserver.com

Pop V. (2011), 'EU commission defends telecoms surveillance law', EU Observer

StateWatch Report (2011), 'Intensive surveillance of "violent radicalisation" extended to embrace suspected "radicals" from across the political spectrum', available on Guardian.co.uk

Kosta E., Kalloniatis C., Mitrou L. Kavakli E. (2011), 'The ''Panopticon'' of search engines: the response of the European data protection framework', *Requirements Engineering,* vol. 16 (1)