Rechtenforum.nl

Egregious use of Tor servers?

Data retention, anonymity and privacy online

Auteur: F.W.J. van Geelkerken

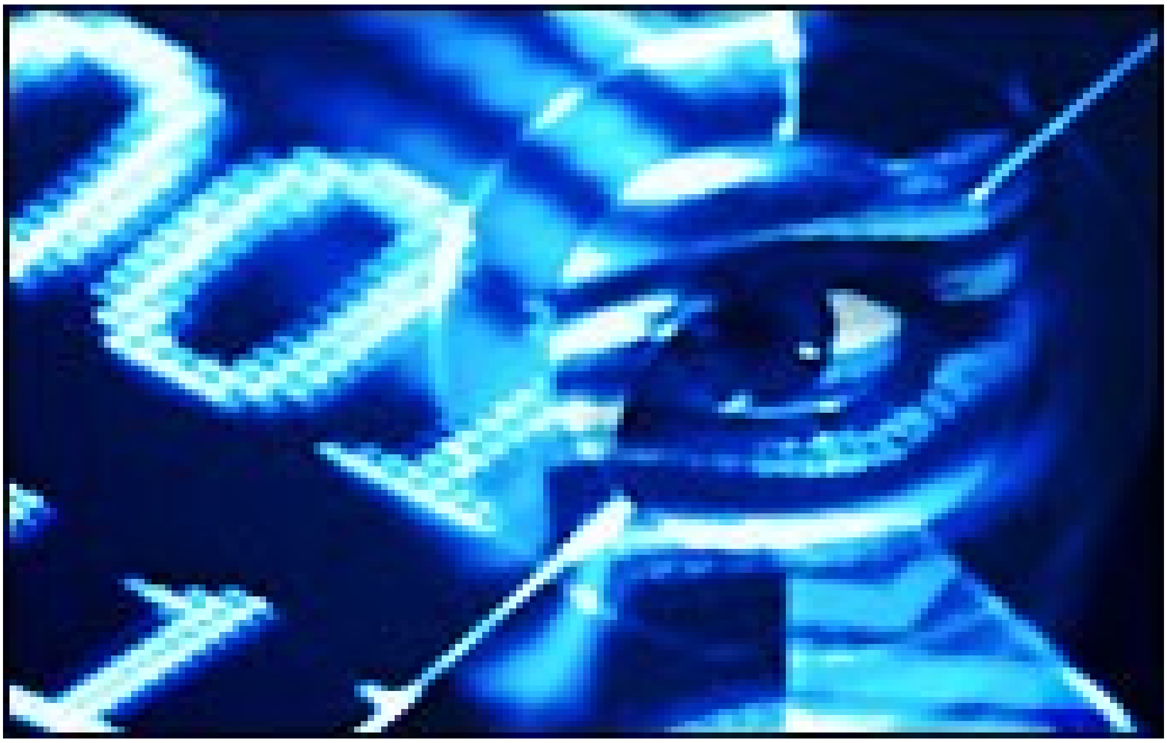


Table of contents

Chapter 1: Introduction

1.1 Introduction

From the early nineties of last century onward the importance of information and communication technology has grown significantly. Not only has the reliance on ICT by most western countries exponentially grown, ICT is also used increasingly to commit criminal acts. To refute the notion that anyone can do anything with a computer, many countries have adopted specific legislation to penalise computer crimes. In the United States these measures did however not have the wanted deterrent effects on criminals committing e.g. computer fraud.[1]

Up to 2001, the emphasis of the legislation in the United States was on the prevention of-, and holding perpetrators accountable for, computer crimes. However, the emphasis changed to also incorporate the preparatory acts for serious crimes after the attacks on september 11th, soon many European countries followed suit. In July 2005, the European Commission made a draft proposal for a directive on data retention, which would make it impossible to be anonymous[2] online. This proposal caused widespread indignation and many groups started petitions against such a directive. These actions were however to no avail because March 15th 2006 the data retention directive was adopted.

On the other hand, Tor, software using a technology called onion routing, enables its users to communicate at various levels of anonymity on the Internet, which goes directly against the objectives of the aforementioned directive. This situation gives rise to the following central question of this paper:

How can and should the European Union and its member states address the problem that the use of Tor poses considering the objectives of the data retention, taking into account the legitimate uses of Tor in the information society?

[1] McCollum 2002.

[2] In the context of this paper the terms anonymity and a high level of privacy are interchangeable.

1.2 Approach

To answer the central question I will split it up into multiple sub questions and answer them in separate chapters. Firstly, in chapter two, what is data retention and what does the data retention directive curtail in theory? In chapter three, what is Tor and what is onion routing, the technique Tor uses? In chapter four, I will give an overview of the data retention directive by expounding on the benefits and risks of the data retention directive in practice. In chapter five I will similarly expound on the benefits and risks of Tor in practice. In the sixth chapter I will describe which forms of regulation are and which are not options for regulating Tor. In the seventh chapter I will make a benefit- and risk evaluation, to give a short summary and answer the central question in chapter eight.

Chapter 2: The data retention directive

In this chapter, I will expound on what the data retention directive[3] is and how it functions, or rather should function, in practice. The objective of the DRD is twofold, instating and harmonising data retention legislation and ensuring the availability of those data for the investigation, detection and prosecution of serious crimes.

However there is no consensus on the specific definition of what data retention exactly is; therefore, I will use the definition given by the DRD. Data is defined in article 2 paragraph 2 section (a) as being traffic[4]- and location[5] data and the related data necessary to identify the subscriber or user. Retention is not specifically defined in the DRD, however based on consideration 15 of 2006/24/EC in conjunction with article 3 2006/24/EC and by derogation of 95/46/EC, it is possible to formulate a definition. Data retention can be defined as being any operation, or set of operations which is performed upon traffic and location data and the related data necessary to identify the subscriber or user,

[3] 2006/24/EC, here after referred to as the DRD.
[4] As defined in article 2 paragraph (b) 2002/58/EC.
[5] As defined in article 2 paragraph (c) 2002/58/EC.

whether or not by automatic means, such as collection, recording, organization, storage, or retrieval.

Based on article 5 of the DRD, several kinds of data need to be retained by providers[6] of publicly available electronic telecommunication services[7]. As only the retention of internet communication is relevant for this paper I will limit myself to this aspect of the DRD. Providers of internet services need to retain the following information; data necessary to trace and identify the source and destination of a communication, data necessary to identify the date, time, duration and type of communication, and data necessary to identify users' communication equipment. When combining these data it is easier for a policing agency, when they subpoena these data, to detect, investigate and prosecute serious crimes because these data, when combined, grant an almost complete view of a subject's online behaviour.

Chapter 3: Tor

In this chapter I will give a very brief explanation of what Tor and what onion routing (the technique that Tor uses) is. Explaining the specific technical aspects of Tor and their respective advantages and disadvantages would be beyond the goal of this paper.[8] I have however added figures to clarify how digital mixing, anonymising proxies and Tor works.

3.1 Theoretical background of onion routing

Chaum's mix-network[9] forms the basis for almost all practical solutions of remaining anonymous online such as onion routing. With the aid of such a mix-network, anonymous communication can be achieved because it is not possible to correlate the messages it receives to the messages it forwards. A mix changes the order, delays and pads the traffic it generates when it communicates. Of course delaying is not a feasible option in the case of real-time or two-way-communication. To circumvent the necessity of a delay a chain

[6] Providers of fixed network telephony, mobile telephony and Internet services.

[7] But what is, and more importantly what is not, to be considered a publicly available electronic telecommunication service in the sense of the DRD is not specified.

[8] For a more in-depth analysis of these techniques see van Geelkerken 2006.

[9] Chaum 1981.

of mixes is necessary, and one way of making such a chain is onion routing.[10] By forming a chain of intermediate entities from the initiator to the recipient of a communication an adequate level of anonymity can be achieved.[11] In the case of Tor these intermediate entities are called nodes, although other onion routing systems simply refer to them routers. These nodes are similar to anonymising proxies, in the sense that they forward the received communication from and to the initiator as shown in the figure on the next page.

3.2 Onion routing in practice

When using onion routing the chain of nodes is formed as follows. The initiator encrypts the data he or she wants to communicate in several layers[12] with the aid of public key encryption and sends it to the first node. The entry node will remove the first layer of encryption and permute the data to the second node. That node will also remove a layer of encryption and send the data to the third node. Every successive node will do likewise until the last node, the exit node, removes the remaining layer of encryption and sends the unencrypted message[13] to the intended recipient as illustrated on page 6 and 7.

Every individual node only knows the identity, IP address, of the previous and the successive node. And only the entry- respectively exit node know the initiator and intended recipient of the communication. Which means it is impossible to correlate the complete communication as long as there are at least three nodes. As long as this chain is changed often enough, or the initiator is part of an other user's chain, onion routing provides a much higher level of anonymity[14] than other privacy enhancing technologies because the degree of

[10] Using crowds or hordes is also possible.
Crowds: Reiter and Rubin 1998.
Hordes: Shields and Levine 2002.

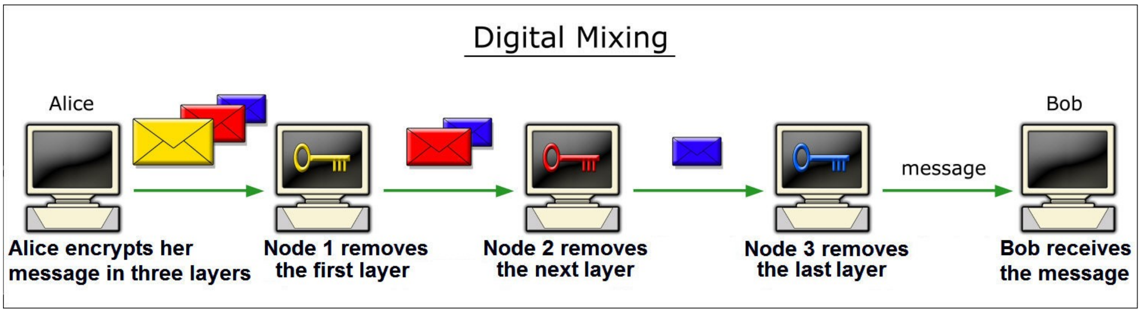
[11] However this does require some form of encryption of the data which is sent and received by respectively the initiator and recipient.

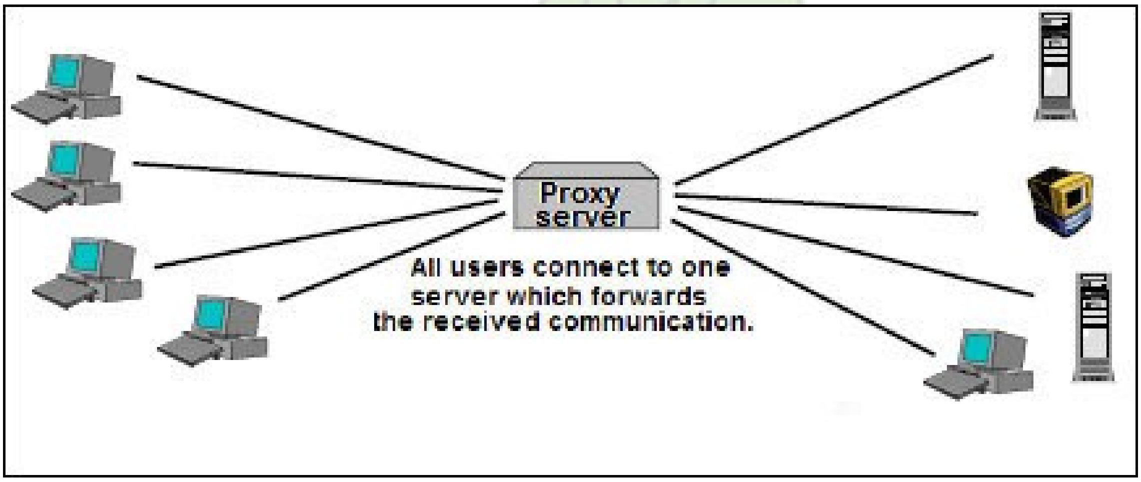
[12] Depending on the software is used more or less layers of encryption are used, Tor normally makes use of three layers of encryption.

[13] The multiple layers of encryption which need to be removed to get to the message gave onion routing its rather peculiar name.

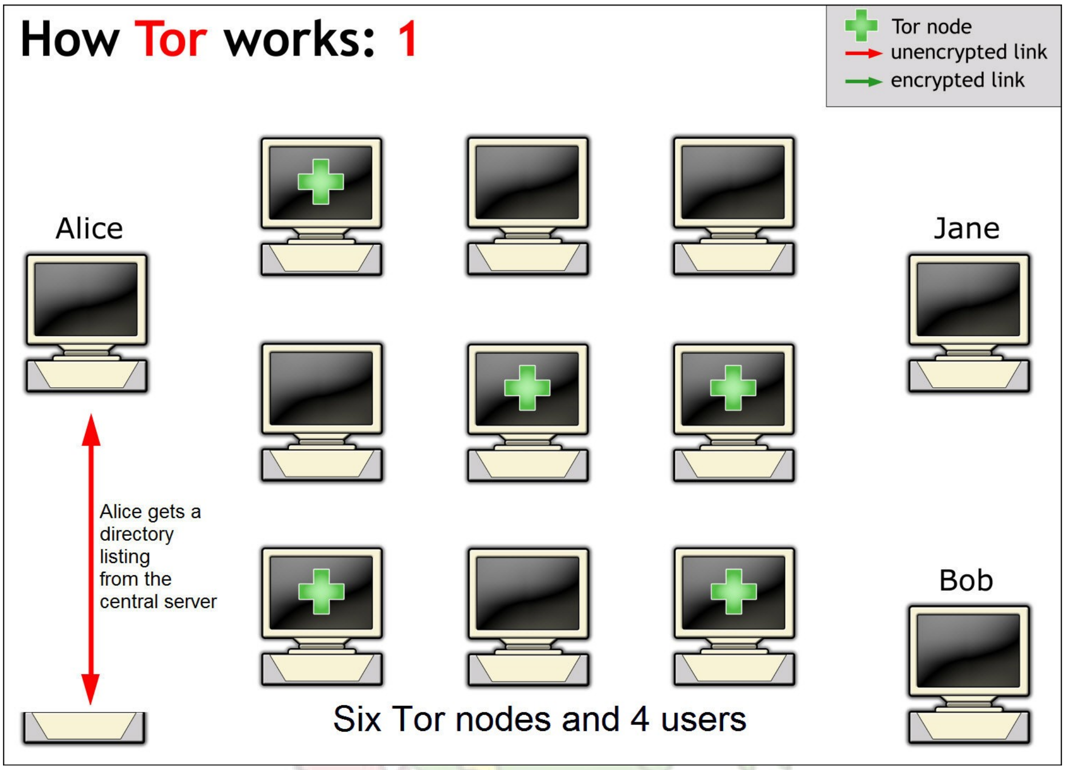
[14] Schneier 2006-1.

linkability[15] of a user is decreased significantly as is illustrated in the last picture on page 7.


Digital Mixing
Alice
Bob
message
Alice encrypts her message in three layers
Node 1 removes the first layer
Node 2 removes the next layer
Node 3 removes the last layer
Bob receives the message


Proxy server
All users connect to one server which forwards the received communication.

[15] Hope-Tindall 2006.



How Tor works: 1

✚ Tor node
→ unencrypted link
→ encrypted link

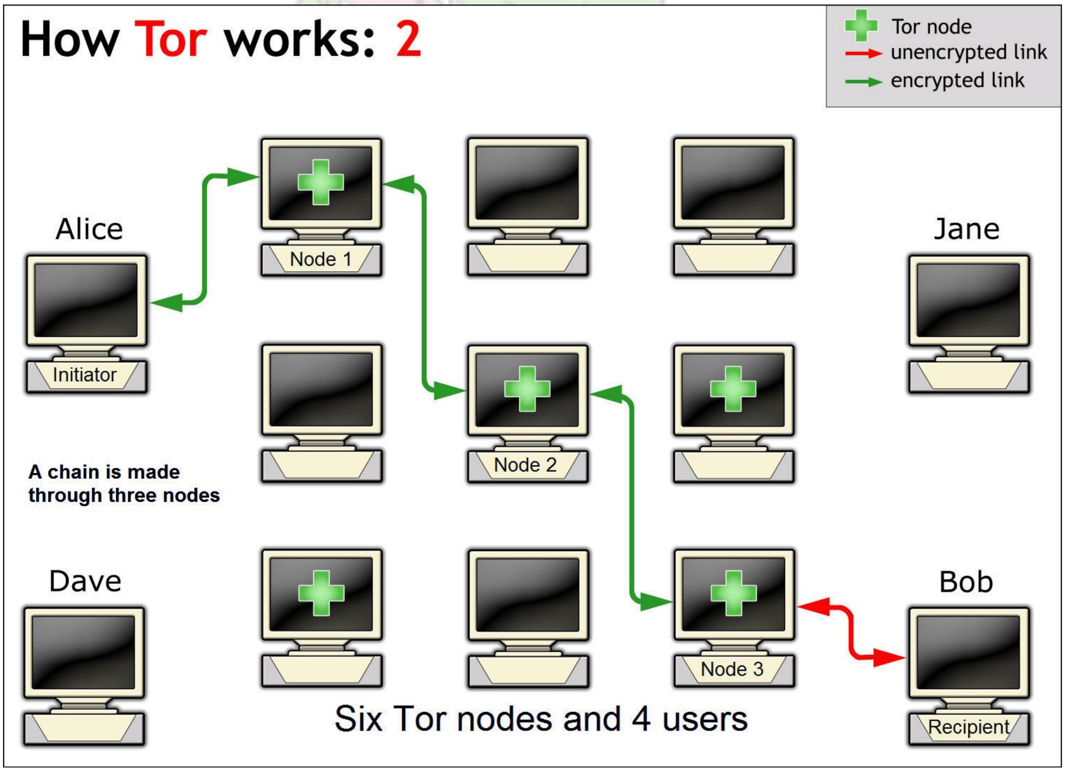
Alice

Jane

Alice gets a directory listing from the central server

Bob

Six Tor nodes and 4 users



How Tor works: 2

✚ Tor node
→ unencrypted link
→ encrypted link

Alice

Initiator

Node 1

Jane

Node 2

A chain is made through three nodes

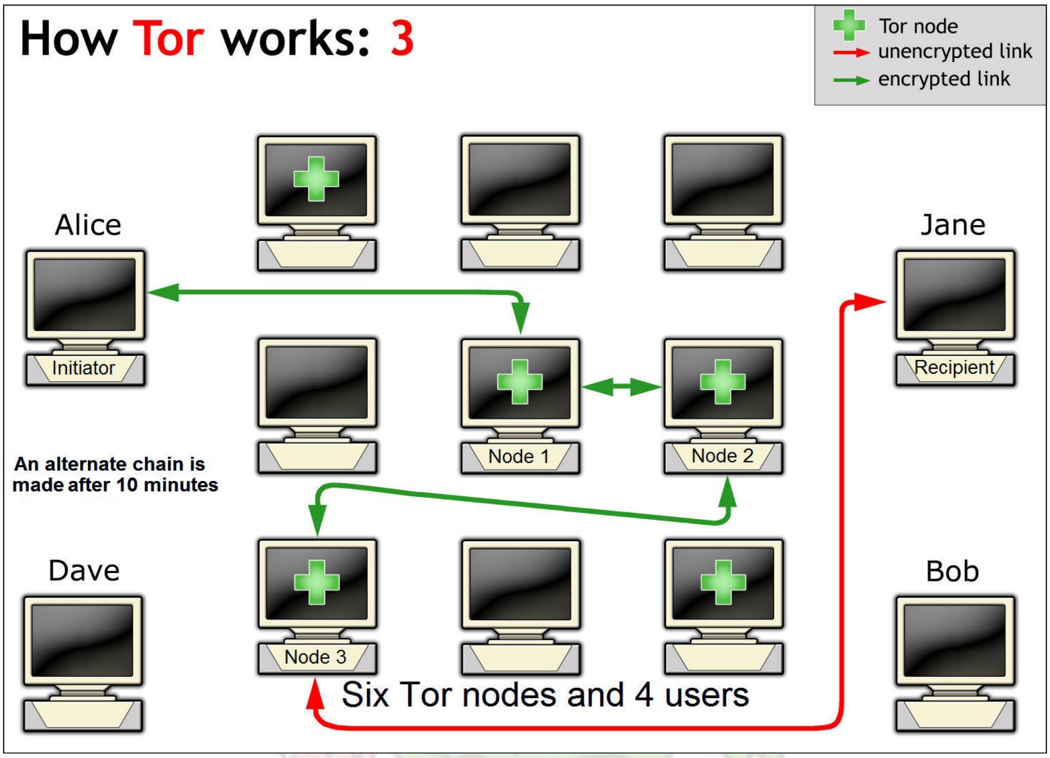
Dave

Node 3

Bob

Recipient

Six Tor nodes and 4 users

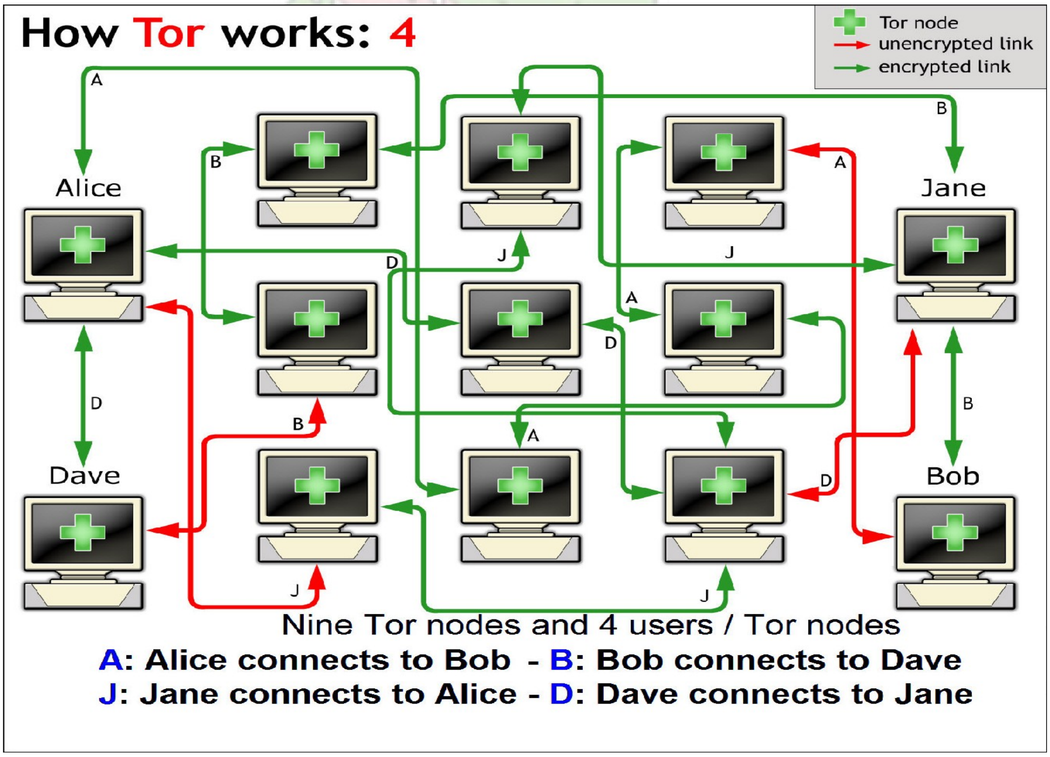


How Tor works: 3

🟩 Tor node
🟥 unencrypted link
🟩 encrypted link

An alternate chain is made after 10 minutes

Six Tor nodes and 4 users



How Tor works: 4

🟩 Tor node
🟥 unencrypted link
🟩 encrypted link

Nine Tor nodes and 4 users / Tor nodes

A: Alice connects to Bob - B: Bob connects to Dave
J: Jane connects to Alice - D: Dave connects to Jane

Chapter 4: The data retention directive in practice

In this chapter, I will expound on the DRD in practice.[16] To achieve this I will first elaborate in paragraph 4.1 on the beneficial affects the DRD can have or has, amongst others for society. In paragraph 4.2 will elaborate on the risks[17] the DRD can have or has, amongst others for law-abiding people.

4.1 Benefits of the data retention directive

Data retention, and by extension the DRD, can have benefits on several aspects of fighting (serious) crimes. To clarify these potential benefits, I will discuss these different aspects and conclude with general benefits.

The first beneficial aspect of the DRD is the fact that these crimes can be detected more easily and in some circumstances earlier. The fact that *all* traffic data of *all* users in *all* member states is retained, means it is unfeasible to detect crimes more easily or earlier simply by analysing these data. Therefore, policing agencies make use of criminal- and crime profiles to detect crimes and (potential) criminals. These profiles can be useful when analysing traffic data, even without there being a suspicion of a certain crime which has been or will be committed, because it makes it possible to establish such a suspicion. This way a policing agency can even find out about crimes such as hacking, or running a network of computers[18]. Without the retention of traffic data such crimes are very rarely detected by policing agencies because they are dependent on the willingness of victim to report the crime, which especially large companies are not eager to do.[19]

Data retention can also be very beneficial for the investigation of crimes, because the DRD makes it possible to find out with whom a suspect has communicated, making it slightly easier to investigate criminal organisations and therefore to find other (potential) suspects. However, data retention also makes it possible for policing agencies to find out (faster) who can be eliminated

[16] The DRD has not yet been implemented up to this point in any member state, which means I will need to rely on the few examples where data retention is legislated, e.g. the United Kingdom.

[17] When I use the term risk I refer to risk as a hazard, Slovic 2002, p. 4

[18] A so called "botnet", with the side note that these kinds of networks are not all used for malicious goals. Schneier 2006-3.

[19] http://www.fox-it.com/content/view/336/99/lang,nl/ (Dutch only) accessed November 11, 2006.

as a suspect for a crime. The fact that the DRD makes it possible to retain data longer can also be beneficial for the investigation of crimes. Especially with serious crimes like murder, and crimes that require extensive investigation like Nigerian “e-mail scams”, the retention of data for a longer time can be beneficial.[20]

The DRD can also be very beneficial to the prosecution of (serious) crimes. Especially in cases where a person is suspected of being part of a criminal- or terrorist organisation, it is very difficult to prove their involvement. However through the retention of telecommunication data it is possible to ascertain *who* communicated with *whom, where* this communication took place and *how long* the communication lasted[21]. The aforementioned facts all make it easier for the public prosecutor to prove beyond a reasonable doubt that a suspect was indeed a part of a criminal- or terrorist organisation.

Without the aid of data retention in many cases the culprit(s) of computer crimes cannot be prosecuted, even if their identity is known, because it is simply impossible to prove that they committed the crime. However, the retention of traffic data has made it easier to prosecute the perpetrators of computer crimes. Instead of a Dutch prosecutor having to find out if it is possible to obtain certain traffic data, if they are even retained at all, the DRD makes it possible to be certain beforehand if such data exists and in what situation it is available and/or obtainable to the prosecutor.

4.2 Risks relating to data retention

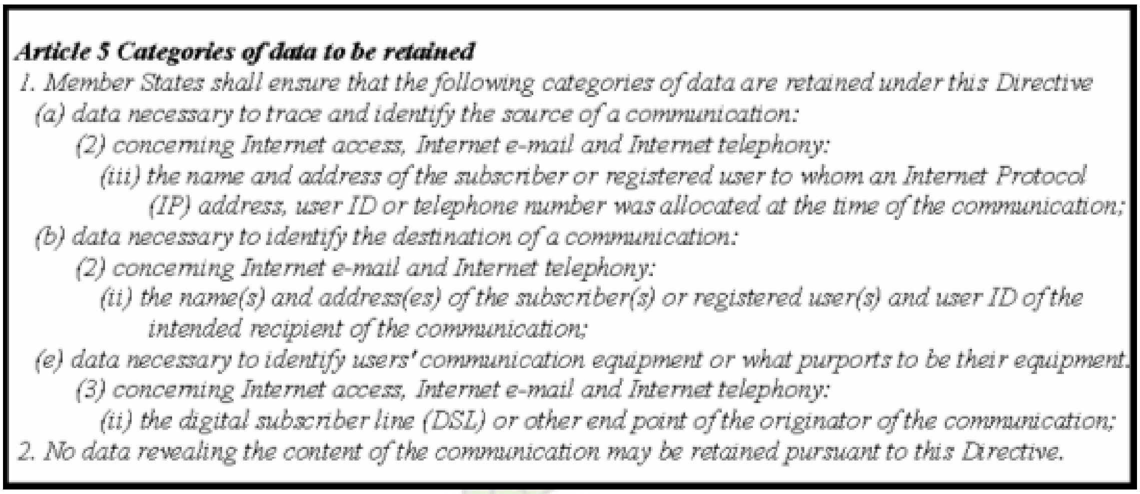
Data retention does not only have beneficial effects, it also creates several risks. I will limit myself to three risks even though many more exist. First of all, data retention can violate the right to privacy[22] as formulated in article 8 ECHR. Even though the DRD specifically mentions this right, and the fact that

[20] For two reasons, first of all the perpetrators of such crimes do more to prevent detection. And secondly, in the case of serious crimes it is necessary to perform lengthy, investigations.

[21] Through the calling telephone number in combination with the IMEI code and the called telephone number.

[22] *The condition of not having undocumented personal knowledge about one possessed by others.* Parent 1983, p. 269.

the DRD complies with the requirements of article 8 paragraph 2 ECHR to limit the right to privacy.[23]



Article 5 Categories of data to be retained

1. Member States shall ensure that the following categories of data are retained under this Directive
(a) data necessary to trace and identify the source of a communication:
(2) concerning Internet access, Internet e-mail and Internet telephony:
(iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;
(b) data necessary to identify the destination of a communication:
(2) concerning Internet e-mail and Internet telephony:
(ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;
(e) data necessary to identify users' communication equipment or what purports to be their equipment.
(3) concerning Internet access, Internet e-mail and Internet telephony:
(ii) the digital subscriber line (DSL) or other end point of the originator of the communication;
2. No data revealing the content of the communication may be retained pursuant to this Directive.

The provisions of article 5, when combined, violate article 8 paragraph 1 ECHR.[24] For, whenever a user communicates through the Internet both the initiators and the end points IP address need to be retained based on article 5 paragraph 1, and paragraph 2 states that it is not allowed to retain information regarding the content of the communication. These two paragraphs do not seem to collide however if Alice connects from q6745.Tilburg.XS4ALL.com to 3XTZ9.stormfront.org[25] a third party would be able to ascertain a lot more information about the initiator and recipient of this communication than only the IP addresses.[26]

A second aspect of the DRD can pose a serious risk, through legitimising the widespread retention of traffic data, there is an increased possibility of governments or policing agencies monitoring groups who are in conflict with the state.[27] This risk is strengthened by the fact that the DRD does not specify, quantify or otherwise make known what should be considered to be “serious crimes”, but instead leaves this up to the individual member states.

[23] The limitation is necessary in the interests of national security, for the prevention of disorder or crime and for the protection of the rights and freedoms of others.

[24] If this violation is mandated through article 8 section 2 ECHR is disputed.

[25] Stormfront.org is a website and forum, famous / notorious for its (extreme) right members.

[26] This would ofcourse still not make it possible to identify the initiator of the communication.

[27] For instance, legitimate protestors against the Iraq-war, and protestors at an arms fair, in the UK.

In extreme circumstances, this could lead to a situation in which similar acts are deemed not criminal, crimes or serious crimes in different member states. In a member state in which a certain political party is deemed dangerous to the state, just because it poses a threat to the established political parties' interests, their traffic data could be subject to investigation.[28]

This brings me to an even bigger risk. Because the DRD does not stipulate specific judicial oversight of the access to the retained traffic data, a less than benevolent member state can make legislation that bypasses any form of judicial[29] oversight[30].

Chapter 5: Tor in practice

In this chapter, I will expound on the use of Tor in practice. To achieve this I will first give a brief description of the makers' or designers' objective(s) for Tor in paragraph 5.1. In paragraph 5.2 I will elaborate on the beneficial effects, the use of Tor can have or has, amongst others for its users. In paragraph 5.3 I will elaborate on the risks the use of Tor can have or has, amongst others for society.

5.1 Objectives of Tor

The makers' or designers' sole objective of Tor was the ability for Tor users to be online without a, possibly malevolent, third party being able to find out *who* is online, to *whom* he or she connects and (partially) *what* they are communicating.[31] Or as they put it *[...]Tor seeks to frustrate attackers from linking communication partners, or from linking multiple communications to or from a single user.*[32]

5.2 Benefits related to the use of Tor

There are three distinct groups of people who can greatly benefit from the use of Tor.

[28] Schneier 2006-2.

[29] The DRD only talks about *public authorities [...] responsible for monitoring [...]* in article 19. A "public authority" does however not necessarily mean there is the possibility of judicial oversight.

[30] Schneier 2006-4.

[31] The protection against third parties knowing *what* is communicated is achieved by using Privoxy.

[32] Dingledine 2004, p. 3.

I will discuss these three groups in paragraph 5.2.1 and conclude with benefits for users based on geographic locations in paragraph 5.2.2.

5.2.1 Groups benefiting from the use of Tor

The largest group of people, which can greatly benefit from the use of Tor, is a group I would like to call “every day people”. Using Tor for them does not have the goal of being anonymous. To them Tor is one of the few effective ways of securing their privacy online.

By using Tor software it is possible for e.g. insiders to act as a whistleblower.[33]

Using Tor software also has many benefits for companies. If in a period of 24 hours fifteen times as many computer programmers as normal browse www.monster.com, an online job site, and they all connect from an IP address belonging to Oracle, a large supplier of ASP systems, this gives the people at www.monster.com a lot of information. It could potentially even be sensitive information, for maybe Oracle is not doing that well or they are reorganising, and if such knowledge is not (yet) available to the general public, it might even lead to insider trading.

The third group that can benefit from the (widespread) use of Tor is governments.

If an intelligence agency, e.g. the Dutch AIVD or the British MI5 wants to investigate or infiltrate a group of people suspected of distributing child pornography it would do them no good to connect with an IP address reading e.g. AC45B569.MI5.GOV.UK. However, if they can use any “normal” IP address (of the exit node at that time) they would not be recognised as easily. Governments could of course also use their own version of Tor. However, this would also not be effective for it would only mean that “a group”, irrelevant of its size, are *all* government employees. The only way policing agencies and intelligence agencies can investigate, infiltrate or otherwise approach a (group of) computer criminal(s), terrorist cell, or other criminal online is to blend into the group of “normal” Internet users.

[33] For instance Enron in the United States and the Dutch fraud in the construction industry.

5.2.2 Geographic locations

Using Tor can also be very beneficial in certain geographic locations, regardless of the fact to which of the aforementioned group the people utilising Tor belong. The use of Tor can be beneficiary for users in the following specific geographic locations; countries with active censorship[34], countries with limited freedom of speech[35] and countries where being a dissident can be life threatening[36].

People "behind" the great firewall of China cannot have access to independent sources of news because those IP addresses and IP ranges are blocked or their DNS is poisoned. However connecting to a Tor node is not prohibited, which means connecting to e.g. Wikipedia sites about the Falung Gong movement is possible. Likewise all Internet traffic is monitored; by amongst others the People's Republic of China and Byelorussia, to be certain no one writes anything that is deemed politically undesirable.[37] Moreover, the possibility to be anonymous online is even more important for dissidents. To make sure that their lives are not endangered unnecessarily while trying to change a society or overthrow a corrupt government, dissidents rely on amongst others Tor to make them untraceable.

5.3 Risks related to the use Tor

The use of Tor does not only have beneficial effects, it also creates several severe risks. First of all, it creates a risk for an increase in computer crimes where the perpetrator remains anonymous. If a potential criminal is certain that he or she can commit a crime, such as phishing or hacking, without the appropriate policing agency being able to ascertain the identity of the perpetrator this might entice that person to commit such a crime. Similarly, distributors of virtual child pornography would abandon their ways of distribution

[34] Amnesty International 2004.

[35] Amnesty International 2006-1.

[36] Amnesty International 2006-2.

[37] According to widespread online rumour, the Internet Society of China (ISC) advised a mandatory registration of webloggers' real names. Luan Shanglin (2006). *Blog real name system not yet officially decided.* http://news.xinhuanet.com/english/2006-10/23/content_5236067.htm accessed October 25, 2006.

in favour of anonymous distribution with the aid of Tor. A second potential risk that the use of Tor might pose is the fact that non-computer crimes and preparatory acts for such crimes will be committed more anonymously with the aid of Tor. Instead of using verbal communication via telephones, terrorist cells might contact each other while both using a Tor client, making them virtual untraceable for any regular policing agency. A third risk, which has already been proven in practice to be possible, is the use of Tor to register a hotmail account to send a ransom note anonymously. Similarly by using Tor any person would be able to send unsolicited e-mail messages, so called Spam, without the possibility of that person being held responsible for the (possible) resulting damages.

Chapter 6: Regulating Tor

In this chapter, I will expound on the possibilities of regulating Tor and the use of Tor. I will do this by first describing in paragraph 6.1 which ways there are to regulate behaviour, to explain in paragraph 6.2 why certain options are not viable ones in the case of Tor and the use of Tor. In paragraph 6.3 I will elaborate on both the reasons why the use of Tor should not be and why it should be regulated (or be deemed illegal) by law in individual member states.

6.1 Regulation of behaviour

There are several ways of regulating behaviour in the offline world, which can be similarly applicable in the online world, albeit in an altered form in certain cases. I will limit myself to four general modalities of regulating behaviour, however each of these can be further defined in many more (sub) modalities.

The most common and oldest way the behaviour of individuals is regulated is the adherence to social norms. To prevent an individual being labelled as social outcast that person will not exhibit certain socially undesirable behaviour. If it is frowned upon when a person smokes in buildings of Tilburg University, that kind of behaviour will not be exhibited. Social norms, and through this self regulation, can be very effective in small(er) communities but will lack effectiveness if such communities grow larger, because the norms will not be internalised and therefore slowly dissipate.[38] That means when social norms do not, or cannot, regulate the behaviour of individuals (enough), other ways of regulating are necessary. Another way of regulating behaviour is regulating by or through the market. By increasing or in some cases decreasing, the (monetary) cost of certain behaviour it is possible to influence the exhibit of such behaviour. If at Tilburg University it is deemed socially undesirable the price of cigarettes sold at the university could be raised.[39] A third modality of regulating behaviour is architecture, meaning the physical surroundings which limit certain behaviour. If it is not possible to buy cigarettes on the campus of Tilburg University this will limit the undesirable behaviour. The fourth and most widely used form of regulating (unwanted) behaviour is the law. By penalising certain behaviour, like smoking in public accessible buildings, this form of behaviour can be regulated.

Lessig also mentions these four modalities of regulation in his 1999 essay,[40] and applies these modalities to the online world, in his words cyberspace, but he substitutes the offline modality of architecture by the term code.

6.2 Viability of different regulatory instruments for Tor

Social norms as regulatory tool have been, and in certain aspects still are, the most common way of regulating online behaviour the last ten years.[41] Similarly the makers of Tor rely on the social norms and common sense of its users.[42] But since users can also use the Tor network for criminal acts, and blocking questionable content is not possible[43], nor desirable[44], and blocking

[38] Eisenberg 1999

[39] The fact that this is not possible in practice is irrelevant to the example.

[40] Lessig 1998

[41] For instance the fact that there was something as called "netiquette" as early as 1995. Website: http://tools.ietf.org/html/rfc1855 accessed November 14, 2006.

[42] EFF 2005.

[43] TorFAQ-1.

[44] If questionable content should be blocked, who would decide what to block and what not?

specific users is not possible[45], regulating Tor based on social norms is not a possibility.

Regulating Tor through or by the market could be possible if Tor were proprietary software. In that case it would be possible to make Tor client- and server software only available to specific government- and policing agencies, eliminating the possibility of a criminal using Tor. However Tor is *not* proprietary software, and even if it were, this would seriously decrease the diversity of the Tor network which could seriously hamper government- and policing agencies in their investigation of serious crimes. This means that regulating Tor through or by the market is not a possibility.

The third option, regulating Tor through architecture, or code as Lessig calls it, could be a viable option. If the designers of Tor were to build in a backdoor, the possibility for specific government- and policing agencies to secure remote access to a computer, in Tor these agencies would still be able to investigate suspects of serious crimes. However the designers state they have not built in[46] such a back door in their software, nor do they think they can ever be forced to do so.[47] If their statement that they cannot be forced to build in a backdoor is true, and I have no reason to doubt this, regulating the use of Tor by changing the code of Tor does not seem like a viable option. However there is a second way of regulating Tor through architecture.

If all access to Tor nodes were to be blocked for regular users, but still be available for government- and policing agencies, the Tor network could not be used by users with criminal intent. But this second, rather drastic, way of regulating is also not an option because of three reasons. First of all this would require ISPs to have very extensive filtering software, secondly this would not prevent users from connecting through a “normal” anonymising proxy and connecting to the Tor network, and thirdly, and most importantly, this would

[45] Considering the fact that every user is anonymous, even for the designers, it is not possible to block certain users from using the Tor network.

[46] TorFAQ-2.

[47] See previous footnote.

significantly hamper government- and policing agencies in being anonymous in the network. This means that the third modality of regulation, regulating Tor through architecture, is not possible.

Since all other ways of regulating Tor and the use of Tor are not viable options only regulation through legislation remains. Since regulation of behaviour through legislation is in principle always possible, as long as this does not violate constitutional- and human rights, regulating Tor and the use of Tor is a viable option.

6.3 Regulating Tor through legislation

There are several grounds why Tor should be legislated or even be illegitimated, and similarly there are grounds why this should not happen. This is why I will expound on the arguments why Tor should and why it should not, be legislated in respectively paragraph 6.3.1 and paragraph 6.3.2.

6.3.1 Why Tor should not be regulated through legislation

I will limit myself to only a few arguments why Tor does not need to be legislated by individual member states, even though many more exist.

The most important reason why Tor should not be specifically legislated, or even be illegitimated, is the fact that it (only) increases the privacy level of the everyday person.

These users are still not completely anonymous, for they still need to use the architecture of the Internet. This means they can still be investigated by placing a wiretap on e.g. their Internet connection.[48] In addition, when utilising Tor the individual user is able to reduce the first of the aforementioned risks of data retention, the violation of his or her right to privacy on the basis of article 8 ECHR.[49]

Secondly using the Tor client software and running nodes makes it possible for people in other member states and third countries[50] to exercise their rights as granted by, amongst others, article 8, 9 and 10 ECHR and article 17,

[48] Investigation *is* possible, albeit considerably more difficult than “simple” traffic data analysis.

[49] If the violation is indeed not mandated through article 8 section 2 ECHR.

[50] Countries not belonging to the European Union.

18 and 19 ICCPR. Moreover, all states party to the ICCPR have, based on article 2 ICCPR, the obligation to respect and to *ensure* the rights granted by the ICCPR. If Tor were to be illegitimated, even if this were done based on, and in accordance with, article 17 paragraph 3 and/or article 19 paragraph 3 ICCPR, this would be a direct violation of the obligation laid down in article 2 ICCPR.

Thirdly national governments, or at least certain of their policing agencies, need a Tor network which is as diverse as possible to be able to do in depth investigations[51], investigations into serious crimes such as terrorism and organised crime. If Tor were to be legislated, or worse be deemed illegal, these policing agencies would no longer be able to remain anonymous for the groups of criminals they would like to infiltrate or investigate, and eventually prosecute.

6.3.2 Why Tor should be regulated through legislation

In this paragraph, I will give three arguments why Tor needs to be illegitimated, or at the least why it should be legislated, by individual member states.

The foremost reason why Tor needs to be illegitimated, or at least legislated, is the fact that a user with criminal intentions can largely nullify the aforementioned positive aspects of the DRD by utilising Tor software. Instead of there being a log of a direct connection, and therefore a fixed and objective evidence of a connection, between an individual user and a certain website or e-mail address, their would be thousands, if not millions, of connections of which policing agencies cannot ascertain which ones were initiated by a particular individual.

The second reason why Tor, or at least running a Tor node, should be legislated is the fact that running a Tor node can hamper the investigation of serious (computer) crimes. The positive effect on the investigation of serious (computer) crimes as mentioned in subparagraph 4.2.2 could be completely voided because Tor makes the investigation and prosecution of serious

[51] "Under cover" investigations.

(computer) crimes more difficult[52], albeit not impossible[53]. When a person runs a Tor node, it is not possible early on in an investigation to eliminate that person as a suspect, or to strengthen an existing suspicion, based on traffic data because those data would not be useable as exonerating or incriminating facts.[54] Moreover, because it is not possible to eliminate or strengthen suspicions earlier in the investigations the whole process of investigating would be delayed unduly.

Thirdly, as I explained in paragraph 3.2 Tor makes use of (strong) public key encryption which makes it possible for e.g. the policing agencies in the United Kingdom to impose a disclosure requirement if certain conditions are met.[55] However disclosing the public key is not possible for a user of Tor or person running a Tor node, and demanding disclosure of a private key is not useful[56], and might in certain circumstances not even be allowed[57].

[52] Different, Donner 2005.

[53] Investigation and prosecution would still be possible in the same way it was before the DRD came in effect.

[54] Even if the retained data would in part corroborate or contradict the polices suspicion or a suspects alibi, it would be impossible to ascertain if the alleged connection was made by the suspect or an unknown third party using the suspects Tor node.

[55] RIPA 2000 s 49 (2) in conjunction with s 49 (1) (a).

[56] This would only lead to the removal of one "layer" of encryption, with possibly 2 layers remaining. It is even dubious based on s 49 (2) (a) RIPA 2000 if a disclosure requirement to a person running a Tor node can be given at all.

[57] Koops 2000, p. 230-232.

Chapter 7: Conclusion

The problem Tor can pose can only be regulated through legislation. Regulation through the market or regulation through code or infrastructure is not possible because onion routing networks are primarily used by people unwilling to give up their hard fought anonymity or privacy, and the third option, self-regulation, is also not viable because it does not stop malevolent users of using onion routing networks.

To answer the central question it is necessary to make an assessment of both the benefits and risks of not regulating Tor. But because it is not possible to ascertain the specific amount of users and/or malevolent users of Tor[58] it is not possible to perform the kind of risk assessment[59] Shrader and Frechete describe in their book[60]. This is the reason why a qualitative risk assessment will have to suffice. It is certain "everyday people" benefit from the use of Tor by being able to secure their privacy online. And both companies and government- and policing agencies *can* benefit from the use of Tor by respectively preventing possibly sensitive information falling in the wrong hands and the ability to perform in-depth investigations. On the other hand it is certain that when a large group of users start using Tor to secure their privacy online this seriously frustrates the goals of the DRD. And users with criminal intent *can* use Tor to achieve a high level of privacy which makes them harder to identify.

In this case the possibility for "everyday people" to secure their privacy online should outweigh the negative effects the use of Tor has and can have. Especially when considering the fact that computer criminals do not need software like Tor to remain anonymous online. Criminals who are capable of committing computer crimes such as hacking, phishing or DDoS attacks do not want to risk using public software such as Tor. These kinds of criminals can just as easily hack into e.g. an Iranian or North Korean computer to use that

[58] In July 2005 the amount of users was estimated at roughly fifty-thousand. Dingledine 2005, p. 29.

[59] A quantitative analysis.

[60] Shrader-Frechette 1985, p. 15-51.

computer to commit their crimes. That way, even if that IP address were to be traced, they can remain completely anonymous. And even if a (less computer savvy) criminal were to use Tor, this still would not mean that he or she cannot be identified. Identifying that person is still possible, albeit a lot more difficult. This is the reason I think the central question should be answered as follows; the European Union and its member states should not address the problem the use of Tor poses by illegitimating or legislating the use Tor or the running of Tor nodes.

Chapter 8: Summary

In the context of this paper data retention is defined as being any operation, or set of operations which is performed upon traffic and location data and the related data necessary to identify the subscriber or user, whether or not by automatic means, such as collection, recording, organization, storage, or retrieval. In chapter two I have described how the DRD (2006/24/EC) harmonises and regulates the retention of amongst other the traffic data of internet use. Based on article 5 of this directive data necessary to trace and identify the source and destination of a communication, data necessary to identify the date, time, duration and type of communication, and data necessary to identify users' communication equipment need to be retained.

In chapter three I have elaborated why through the harmonisation of data retention obligations on providers of public electronic communication networks, the detection, investigation and prosecution of serious crimes is made considerably easier. Data retention can however also infringe on the right to privacy as formulated in article 8 ECHR.

In chapter four I have described how onion routing, the technique Tor uses, makes use of multiple layers of encryption and multiple rerouting nodes to achieve a high level of anonymity. In chapter five I have described that using a system of multiple rerouting nodes makes the objective of the DRD, the detection, investigation and prosecution of serious crimes, more difficult if not impossible. Onion routing can also be used by government- and policing agencies to perform in depth investigations to infiltrate in otherwise difficult infiltratable criminal- and terrorist organisations.

In chapter six I have elaborated on the four ways of regulating behaviour both offline and online as formulated by Lessig. Regulation can take place through social norms, the market, architecture/code and legislation. I have showed why regulation of Tor through social norms, the market or architecture/code is not a viable option, which means legislation is the only option to regulate Tor and its use. In paragraph 6.3 I have given grounds as to why Tor should, and why it should not, be legislated. The foremost reason why it should not is that, without an onion routing network as diverse as possible, government- and policing agencies cannot perform in-depth investigations as successfully as they currently can. And the fact that, through the widespread use of onion routing networks like that of Tor, the goals of the DRD cannot be reached is the most important reason to legislate Tor.

Chapter 9: Lexicon

9.1 Literature in print

1995/46/EC
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [1995] OJ L281/0031–0050.

2002/58/EC
Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. [2002] OJ L201/0037–0047.

2006/24/EC
Directive 2006/24 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. [2006] OJ L105/0054–0063.

Chaum 1981
David L. Chaum. *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms,* (1981) 24-2 Communications of the ACM.

Eisenberg 1999
M.A. Eisenberg, *Corporate law and Social norms*, (1999) 99-5 Columbia Law Review 1260.

Koops 2000
B.J. Koops, *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?*, (2000) 31 ITeR 230-232.

McCollum 2002
T. McCollum, *Cyber-crime still on the rise,* (2002) in Computer Crime and Security Survey 2002, June 2002.

Reiter and Rubin 1998
M.K. Reiter and A.D. Rubin. *Crowds: Anonymity for Web Transactions,* (1998) 1-1 ACM Transactions on Information and System Security 66.

RIPA 2000
Regulation of Investigatory Powers Act 2000

Parent 1983
W. A. Parent, *Privacy, Morality, and the Law,* (1983) Philosophy and Public Affairs, Vol. 12, No. 4. pp. 269-288.

Shields and Levine 2002
C. Shields and B.N. Levine. *A Protocol for Anonymous Communication Over the Internet,* (2002) 10-3 Journal of Computer Security 213.

Shrader-Frechette 1985
K.S. Shrader-Frechette, *Risk analysis and scientific method: Methodological and ethical problems with evaluating societal hazards,* (1985) Dordrecht, Boston, Lancaster: Reidel, 1985. pp. 15-51.

9.2 Online literature

Amnesty International 2004
Amnesty International, *People's Republic of China: Controls tighten as Internet activism grows.* (2004)
http://web.amnesty.org/library/pdf/ASA170012004ENGLISH/$File/ASA1700104.pdf
Accessed October 25, 2006.

Amnesty International 2006-1
Amnesty International, *Belarus: Valerii Levonevskii and Aleksander Vasiliev were imprisoned for publishing a poem*. (2006)
http://web.amnesty.org/library/Index/ENGEUR490092006?open&of=ENG-BLR.
Accessed October 25, 2006.

Amnesty International 2006-2
Amnesty International, *Belarus: Tightening the screws on dissent,* (2006)
http://www.amnesty.nl/voor_de_pers_artikel/5609.
Accessed October 25, 2006.

Dingledine 2004
R. Dingledine, N. Mathewson and P. Syverson, *Tor: The Second-Generation Onion Router*, (2004) Proceedings of the 13th USENIX Security Symposium, august 13th 2004.
http://tor.eff.org/svn/trunk/doc/design-paper/tor-design.pdf Obtained November 20, 2006.

Dingledine 2005
R. Dingledine, *Tor: Anonymous Communications for the United States Department of Defense...and you,* (2005) Presentation given at Whatthehack, July 29th 2005.
http://freehaven.net/~arma/wth1.pdf Obtained November 20, 2006.

Donner 2005
P.H. Donner, *antwoorden op de vragen over de voorgestelde bewaarplicht van verkeersgegevens*, (2005)
http://www.minjus.nl/images/bewaarplicht%20verkeersgegevens_4471_tcm34-14443.pdf Obtained November 21, 2006.

EFF 2005
Electronic Frontier Foundation, *Legal FAQ for Tor Server Operators* (2005)
http://tor.eff.org/eff/tor-legal-faq.html accessed November 20, 2006

van Geelkerken 2006
F.W.J. van Geelkerken, *Onion routing* (2006)
http://www.iusmentis.com/society/privacy/online/onionroutingintro/
accessed November 20, 2006

Hope-Tindall 2006
Peter Hope-Tindall, *Privacy Enhancing Technologies (PETs): The good, the bad and the possible*, (2006) presentation at the Privacy in the Public Sector: Challenges and Solutions conference, http://www.gov.mb.ca/chc/privacy/presentations/06.pdf
Retrieved 16 November 2006.

Lessig 1998
L. Lessig, *The laws of cyberspace*, (1998)
http://cyber.law.harvard.edu/works/lessig/laws_cyberspace.pdf retrieved November 21, 2006.

Schneier 2006-1
B. Schneier, *Anonymity won't kill the Internet*, January 12, 2006, http://www.wired.com/news/columns/0,70000-0.html Accessed November 21, 2006.

Schneier 2006-2
B. Schneier, *The eternal value of Privacy*, May 18, 2006, http://www.wired.com/news/columns/0,70886-0.html Accessed November 21, 2006.

Schneier 2006-3
B. Schneier, *How bot those nets?,* July 27, 2006, http://www.wired.com/news/columns/0,71471-0.html Accessed November 21, 2006.

Schneier 2006-4
B. Schneier, *Why* Everyone *Must Be Screened*, October 5, 2006, http://www.wired.com/news/columns/0,71906-0.html Accessed November 21, 2006.

Slovic 2002
P. Slovic, E.U. Weber, *Perception of Risk Posed by Extreme Events,* (2002)
http://www.ldeo.columbia.edu/CHRR/roundtable/slovic_wp.pdf
Obtained November 20, 2006.

TorFAQ-1
---- *The Onion Router / TorFAQ: You should change Tor to prevent users from posting certain content.* (2006)
http://wiki.noreply.org/noreply/TheOnionRouter/TorFAQ#FilterContent
Accessed November 22, 2006

TorFAQ-2
---- *The Onion Router / TorFAQ: Is there a backdoor in Tor?* (2006)
http://wiki.noreply.org/noreply/TheOnionRouter/TorFAQ#Backdoor
Accessed November 22, 2006

BBC 2003-1
BBC News, *Rights abuse claim at airbase,* (2003)
http://news.bbc.co.uk/1/hi/england/gloucestershire/3069411.stm
Accessed November 20, 2006.

BBC 2003-2
BBC News, *Police questioned over terror act use*, (2003)
http://news.bbc.co.uk/2/hi/uk_news/england/london/3097150.stm
Accessed November 20, 2006.