ISSA Proceeding 2006 – Hidden Obstructions In Discussions Involving Conductive Argumentation. Core And Surface In The U.S. Debate On The Use Of Data Mining Techniques In The Fight Against Terrorism

Abstract

This article examines some obstructions to adequate discussion that reside not so much at the level of dialectic procedure, but rather at the level of content and motivation. Such obstructions may arise particularly easy when a discussion involves conductive argumentation, and both discussants have reasons for partially or totally suppressing the discussion of certain aspects, in spite of their relevance to the issue at stake. Such jointly agreed suppression does not formally violate the pragma-dialectical rules, since these rules focus on fairness. As an illustration, an analysis is presented of a US debate on the use of data mining against terrorism. Here two potential obstacles of the nature described above can be observed:

(i) There is an ambiguity in the way the issue of privacy tends to be conceptualised.

(ii) Even though the trustworthiness of government agencies is at the core of the issue, there is sometimes a certain reluctance to explicitly address this aspect.

1. *Discussion failures and obstructions*

Discussions are not always as good or as productive as they could be. The reasons for this can reside at various levels:

(i) Certain reasonable principles or standards for discussions are violated by the discussants (*failure of procedure*).

(ii) Certain arguments that are highly relevant to the issue under discussion are

marginalised in the actual debate, or even totally ignored or suppressed (*failure of content*).
(iii) The discussants are driven by motivations that make them less than willing to address certain 'faults' in the discussion (f*ailure of attitude*).

An analysis restricted to level (i) addresses no more than what is put forward by the discussants themselves – augmented perhaps with some obvious and uncontroversial background assumptions not explicitly stated. The only 'faults' identified then will be violations of formal or logical rules concerning the line of reasoning or concerning the procedure of the discussion. It sometimes happens, however, that certain relevant arguments or issues remain unduly marginal in the discussion, are insufficiently addressed or, worse, not stated in any recognizable form at all. This can be due to negligence. It may also be the case that all participants in the discussion have motives that make them forsake these particular aspects. As an example of the latter, take environmental issues. As soon as concrete measures for improving the environment are to be discussed, most actors have a strong incentive to duck the issue: consumers are reluctant to give up their pleasures, industry fears costly changes that could mean a set-back in the international competition, politicians refrain from advocating unpopular measures, and so on (Birrer, 2004; 2001b).
When the discussants themselves fail to sufficiently discuss (or even fail to discuss at all) certain arguments or issues that are highly relevant to the subject of discussion, such failure will be hard to address when the analysis is restricted to level (i), since such an analysis is forced to remain relatively blind to issues of content – and even more so, of course, when that content is entirely missing in the actual discussion. If it is possible at all to address such a failure at level (i), this is likely to require a long chain of interrogating questions of clarification addressed by the analyst to the discussants, since the analyst can only point to the violation of rules rather than directly enter into the content matter itself. When the discussants are consciously or unconsciously motivated to avoid the issue, the situation is still worse, since the indirectness of the analyst's approach makes it easy to evade by the discussants.
It looks like in such cases attempts to improve the discussion should put the discussion in a broader perspective, including levels (ii) and (iii). Even if one's single aim would be to understand what happens in the discussion, it could still be held that such an understanding is incomplete if it does not include an understanding of why the discussion proceeds in the way it does rather than in

another, and that therefore it cannot ignore the aspects under (ii) and (iii).

In the next sections, I will illustrate obstructions at level (ii) and (iii) in more detail for a recent discussion in the US on the use of certain computer techniques in the fight against terrorism. More in particular, I will analyse the arguments that can be found in one specific report on this subject. The issues and arguments that I want to address are all in the report, including what I will identify as the "core issue", so in this case I need not bring in any new arguments or issues that are not already mentioned by the discussants themselves. The potential obstacles to productive debate, however, can be clearly recognised in the arguments in the report – as well as elsewhere in the debate on this issue. The case can thus serve as an illustration of the importance of the broader perspective for understanding the discussion process and for a realistic view on the opportunities for improvement. In the final section, I will return to a few more general questions regarding analysis at level (ii) and (iii).

2. *Data mining to combat terrorism*

Broadly speaking, the term "data mining" refers to a collection of computer science techniques to extract "implicit" information from (large) databases.**[i]** The word "implicit" means that the information to be delved up goes beyond the answers to standard queries (questions that can be formulated straightforwardly in the language of the data base, and that the data base was designed to answer). As an example, think of a database containing administrative data on an organisation's employees. Standard questions for such a database will be: what is the salary earned by Mrs. X, what is her function, what is her home address, etc. A very different use of the database, and usually not one for which the database was originally intended, would be the following. Suppose management is worried about low job performance due to private alcohol and drug abuse. On the basis of the set of those employees who have already been identified as having an alcohol or a drug problem, the board could ask the computer systems department to write a program that searches for predictors, i.e., personal characteristics for which alcohol or drugs problems are above average. Maybe such a program would find that the group with already identified alcohol or drugs problems contains a bigger percentage of unmarried male employees living in a particular area of town than the population of employees as a whole. The board might then wish to scrutinize *all employees with these characteristics*. The board could also wish to prevent that any more persons with such characteristics are hired.

Quite similar methods can be employed in the fight against terrorism. E.g, one might try to find characteristics in the data on terrorists, or characteristics for terrorist activities, and then search for all persons or activities that match those characteristics and have not yet been identified as terrorist. Such automated searches can be applied to ordinary databases, but also to communicative exchanges such as emails, or even telephone conversations. Another possibility is to start from persons and activities that are already suspect, and then use computer information to trace their connections to other persons and activities.
Since the information has to be retrieved from sources that were not originally set up to answer these questions, special programs have to be constructed, and not every question may be answerable. Often it is hard to separate between the relevant and the irrelevant (useful signals/patterns vs. noise): either one finds too many patterns, or hardly any at all. Sometimes information from different databases must be combined, necessitating the coupling of these databases; this may present additional technical problems. However, with the parameters of the search rightly set, the search may be successful. Today, data mining techniques are included in a wide range of US governmental programs, for purposes such as financial accounting, service improvement, analysing scientific information, and the combat of crime and terrorism (for an overview, see GAO, 2004).

Early 2002, in the wake of 9/11, the Defense Advanced Research Project Agency (DARPA) announced a program that was then called "Total Information Awareness" (later the name was changed into "Terrorist Information Awareness"). The program was intended to explore and develop computer science techniques for combating terrorism, data mining being one of these techniques (but by no means the only one). Though right from the start some critics judged the information that DARPA had provided on the program to be insufficiently detailed or clear, it was not until a column by famous New York Times columnist William Safire appeared in November 2002 that a massive and vigorous discussion took off.
Although the program included many other computer science techniques, the discussion almost exclusively focused on data mining. Within a few months the debate had resulted in a moratorium on data mining imposed by the Congress, on January 16, 2003. Secretary of Defense Ronald Rumsfeld installed the TAPAC committee to examine the use of 'advanced information technologies to identify terrorists before they act' (TAPAC, 2004, p. 1). A new report by DARPA, published in May 2003 (DARPA, 2003) was unable to turn the tide. The funding of TIA was

terminated by Congressional decision on September 25, 2003. TAPAC published its report in March 2004 (TAPAC, 2004). It is the argumentation presented in the latter report that forms the main material for the following case study.

3. *The Tapac Report: a brief overview of its content*

In addition to the main text, the report contains a minority report by committee member William T. Coleman, Jr., who disagrees with the main text on several points. The main text refers to Coleman's statement and vice versa, which makes the report a kind of microcosm for the debate as a whole, and a useful source of arguments from both sides.**[ii]**The report also contains a brief separate statement by Floyd Abrams, which basically is another defense of the main report's arguments against Coleman's criticism, and which will not play a role in the analysis presented below.

Following the introduction, the main text contains five sections. The first sections sets out "the new terrorist threat". The second describes the TIA program and the way it was introduced. The third section elaborates the issue of privacy from a mainly juridical point of view. The fourth section analyses the various privacy risks presented by government data mining. The fifth section contains the conclusions and recommendations. My analysis of the main text will focus on the third and fourth section (where the main points of debate can be found), with occasional reference to the other sections.

Brief summary of the section 'Informational privacy and its protection from intrusion by the government'

This section discusses privacy considerations in American law. The main source of privacy protection discussed is Amendment IV of the Constitution that reads 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized'. The protection of citizens is not absolute, as is illustrated by a ruling by the Supreme Court in 1976 that this amendment does not apply to information held by a third party. This verdict is read by the authors of the main report as relating to information that is provided voluntarily, and since much information provided to the government is not really provided voluntarily, they argue that Amendment IV still applies there.

Brief summary of the section 'Privacy risks presented by government data mining'

The section observes that 'Government data mining concerning U.S. persons presents risks to informational privacy which are not adequately addressed by existing law'. (TAPAC, 2003, p. 33). Six main types of such risks are identified:
– *Data inaccuracy risks*. Data may contain errors, different persons with the same or very similar name may mistakenly be identified, etc.
– *False positives.* Since patterns found are merely statistical correlations, part of the identifications (e.g. as a potential terrorist) under such patterns will be mistaken.
– *Data processing risks*. Access-authorized persons may use information in ways not intended by the organisation.
– *Mission creep.* Goals and practices may gradually shift in directions that were not originally intended.
– *Chilling effects and other surveillance risks*. The presence of surveillance activities may negatively affect the general atmosphere in society.
– *Data aggregation risks.* Combination of information from different databases, transnational data flow, etc. may pose additional risks.

Brief summary of the section 'Conclusions and recommendations'
The main report closes with a number of recommendations to curtail these risks, including: that a regulatory framework and oversight mechanisms shall be installed; that the rate of false positives shall be "acceptable in view of the purpose of the search" and that there shall be a system for dealing with false positives; that access to federal databases shall require a written warrant by a federal magistrate or judge; and that the Department of Defense shall yearly publish reports accessible by the public.

Main elements of the 'Separate statement of William T. Coleman, Jr.'
Informational privacy. Coleman thinks that the main report takes the Fourth Amendment too absolute. He agrees that there should be some restrictions on the use of data, but he holds the opinion that the urgency of the battle against terrorism is not taken seriously enough in the main report.
Privacy risks. Coleman stresses that DARPA is a professional organisation that can handle its responsibilities to a larger extent than suggested in the main text, and that therefore too many restrictions are both unnecessary and impeding the fight against terrorism.
Recommendations. Coleman's disagreements with the main report here include that the Department of Defense should not publicly report, but only to some

special committees, and that access to federal databases should not require a written warrant.

4. *Analysis of the arguments*

Privacy and law

First obstruction: the framing of the privacy issue

The section on informational privacy opens with the following remark on the notion of privacy:

"There is a surprising lack of clarity about what "privacy" means and the role the government should play in protecting it. This is due in part to the fact that the word "privacy" is used to convey many meanings. The Supreme Court alone has used the term to describe an individual's constitutional right to be free from unreasonable searches and seizures by the government; the right to make decisions about contraception, abortion, and other "fundamental" issues such as marriage, procreation, child rearing, and education; the right not to disclose certain information to the government; the right to associate free from government intrusion; and the right to enjoy one's own home free from intrusion by the government, sexually explicit mail or radio broadcasts, or other intrusions." (TAPAC, 2004, p. 21)

One of the main problems is the conflation of two separate issues: *access* to information and the *use* made of that information (Birrer, 2001b). When the notion of privacy originally entered the juridical sphere, it referred to the intrusion of the private life of (famous) individuals such as film stars by photographers, journalists, etc. This led to the idea of a "private sphere" that should be free of uninvited intrusion by anyone. Since knowledge of the private sphere of celebrities can hardly be proclaimed as an urgent public interest (notwithstanding the existence of a considerable market for such information), the delineation of such an unassailable private sphere is not likely to meet substantial public controversy. In issues of privacy as the term is used today, the situation often is less simple. Usually, trade-offs are involved between the interest in gathering and using information on individuals on the one hand, and the interests of the individuals concerned on the other. These trade-offs, in turn, do not so much depend on the *access* to the information as such, but on the *use* that is made of that information. This applies to both sides of the balance: the use of the information may serve an important goal that justifies the suspension of certain privacy concerns, whereas it may also be the very ground of certain

privacy concerns in view of the consequences for individuals whose information is (accessed and) used.

The possibility of trade-offs already enters the picture in the formulation of the Fourth Amendment: the term 'unreasonable searches' seems to suggest that acceptability might depend on the goal of the search.**[iii]** In many instances of discussions on privacy issues, however, the intended or actual *use* of the information is not much considered, or not even addressed at all.

There are several possible explanations for the persistence of the conceptualisation of privacy in terms of access only. One obvious reason is historical: since it has been the dominant conceptualisation for such a long time, one might fear that a sudden change of terminology could easily create confusion. Another possible reason is the central position of rights in the language of law. But there could also be a more specific reason for adhering to this kind of framing, particularly for those opposing intrusion of privacy: framing privacy in terms of more or less absolute rights blocks the road towards tradeoffs that could shift in favour of the powerful actors, at the expense of the ordinary citizen. For blocking such 'slippery slopes', a deontological (rule-based) perspective might be seen as more effective than a utilitarian one.

So the situation is that privacy discussions are suffering from a somewhat ambiguous and often misleading framing. Whereas the juridical discussion in this section of the report is important for identifying the possible juridical instruments to provide protection vis-à-vis certain 'privacy' concerns, and can also provide a certain amount of legitimation for privacy concerns in general, it is not to the full extent addressing the question why specific activities would be deemed acceptable or not. Neither the authors of the main report nor Coleman seem to be willing to defer their judgement merely to what the law says or what judges decide; what is really at issue for them is what would be acceptable or reasonable, taking all interests involved into account.

Privacy risks

Second obstruction: the issue of trustworthiness

Once we have understood these limitations and ambiguities of the privacy discussion, it becomes easy to see why the report's next section suddenly starts talking a very different language by considering the risks posed by the gathering, but most of all by the *use* of information on individuals.

What is particularly notable with respect to the privacy risks identified in the

main report is that most of them do not originate in the technique as such, and not even in the use of those techniques as intended. The majority of the risks are 'social risks', referring to consequences not originally intended that result from the 'social dynamics' that may emerge when potential or actual information gatherers or users meet with certain opportunities. This aspect of social dynamics is particularly clear in the case of "mission creep", but it is also an inextricable part of the issue of dealing with "false positives" and of what are called "data processing risks"; it also plays a slightly more indirect role in "data aggregation risks", and more indirectly also in the consequences of "data inaccuracy risks; "chilling effects" rather refer to the social dynamics of society as a whole.

It is this issue of what I called "social risks" that gives us a clue of where the basic difference of opinion between the main report and Coleman really lies: the latter is conceding more trustworthiness to DARPA and the special agency that was to conduct TIA than the authors of the main report. Coleman as well as the main report mainly speak in general terms about their reasons. This is not surprising, of course, since there can hardly be any specific evidence on a program that has yet to start.

Some case-specific arguments are provided in the main report's extensive analysis of the way TIA was announced and explained by DARPA, concluding that TIA "was flawed by its perceived insensitivity to critical privacy issues, the manner in which it was presented to the public, and the lack of clarity and consistency with which it was described" (TAPAC, 2004, p. viii), to the result of seriously undermining DARPA's and the program's credibility. Coleman is more generous (though not completely uncritical) regarding the way DARPA handled the introduction of the program (see Coleman, 2004, p. 81).

For the rest the main report refers to other cases where risks such as the ones described did indeed materialise, cases where courts acknowledged privacy concerns, etc. As mentioned earlier, Coleman pictures DARPA as a professional organisation that can, and for the sake of the effectiveness should, have more autonomy than acknowledged in the main report.

The difference in viewpoint is perhaps most aptly portrayed when Coleman ironically remarks:

"Perhaps I am still misled by the fact that in my youth my parents taught me that policemen on the beat and other law enforcement officers are friends, not enemies, and in my life, most often, it has turned out that way." (Coleman, 2004, p. 74)

Coleman and the main report do not disagree that the fight against terrorism has a very high urgency. They do not even explicitly disagree on the acceptability or unacceptability of certain potential consequences for citizens (although they might have if they had discussed concrete examples). Their main point of disagreement concerns to what extent certain institutions can be entrusted with certain responsibilities, and which checks and balances are needed to contain the potential danger of misuse of these responsibilities.

It often occurs that matters of trustworthiness are avoided – even when they are at the core of what is at issue-, especially when the parties are not yet in total war with each other. Several reasons can be conceived that could account for this phenomenon:
– Questioning the trustworthiness of a person or an institution has a flavour of inappropriateness, as a personal attack, or as an ad hominem argument.
– When a person or institution denies an accusation of lack of trustworthiness, such a denial is hard to conclusively disprove; therefore, the accusation is also easy to evade.
– Suggesting lack of trustworthiness might trigger conflict; conflict-averse persons will try to avoid this by not explicitly addressing it at all.
– For some the possibility of being cheated by someone else might feel as an assault on their self-esteem, making them want to avoid the issue.

These reactions are all very recognisably human, but they may sometimes stand in the way of addressing the issue at stake. Trustworthiness issues occur every time we have to trust a person or institution because we cannot personally monitor it. This happens whenever we depend on scientific experts for information or advice (cf. Birrer, 2001a; see (Birrer, Mentzel, 2005) for an analysis of discussions on biotechnology in terms of trustworthiness). Lay persons lack the expertise to check such information or advice. But the expert need not be a *scientific* expert. The recurring discussion on the adequateness of the information provided preceding the Iraq war is an illustrative example that turns around the reliability of what 'insiders' tell us. Our societies have not yet fully maturated practices to face up to issues of trustworthiness, and to handle them smoothly and effectively. But they will simply have to. The trustworthiness of information and advice is bound to be a core issue in this century; new political equilibria vis-à-vis information asymmetries will have to be established.
Another factor leading to neglect of the issue of trustworthiness, and more

specific to the subject of this particular case study, is what I would call the 'distrust paradox': in organisations with a mission that implies a certain amount of distrust towards the external world there often is a remarkable lack of awareness of the possibility of untrustworthiness of its members, particularly regarding their behaviour towards the outside world. Whereas the mission of certain organisations may necessarily presuppose some amount of distrust towards the outside world, such distrust, if unguarded, can lead to excessive polarisation between 'us' and 'them'. When the issue of terrorism is concerned, we have to be aware that it contains many intricacies, starting with the lack of an agreed definition of what counts as terrorism (Alexander, 2001; Whitaker, 2001), intricacies that provide an effective breeding ground for phenomena like mission creep.

It should be noted that the framing of privacy in terms of access only and the avoidance of the trustworthiness issue are not completely unrelated: concerns about the *use* that can be made of information puts the trustworthiness more prominently into the foreground; as long as privacy is framed in terms of mere access, the issue of trustworthiness is more easily avoided. Even the critical comments by an organisation like the American Civil Liberties Union (ACLU, 2003) are cast partly in terms of access, partly in terms of use (particularly the issue of false positives), and the trustworthiness issue is mainly addressed under the relatively general notion of 'mission creep'. On the other hand, even Safire's column, which most emphatically (and most polemically) exploits the theme of trustworthiness – not only regarding government as a whole, but also regarding the foreseen director of the program -, refers to a panoptic government knowing everything about its citizens rather than explicitly pointing at concrete ways in which the government might misuse that information (although it could be argued that his Orwellian rhetoric is more than enough to evoke the latter) (Safire, 2002).

5. *Collective failures of content and motivation*

The arguments discussed above tend to be belong to the category of conductive arguments (non-conclusive arguments with multiple premises, see (Govier, 1987)). In conductive argumentation, because of its very nature, it is relatively easy to inconspicuously push certain premises and their role further into the background than an assessment of the issue at stake seems to allow, or even to ignore such elements altogether. When one of the discussants commits such a failure, and the failure is to the disadvantage of the other discussant, the other discussant has the opportunity to address it; when it is to the advantage of the

other discussant, on the other hand, the first discussant simply made a strategic mistake that the second discussant may or may not correct. However, as we have seen, it can also be the case that *both* discussants consciously or unconsciously prefer some aspects to be suppressed, i.e., that the failure is a *collective* one.
There is a wide range of possible motivations that may be the origin of such collective failures. One reason is a historical one: a mode of analysis that has been used for a long time gradually becomes less adequate to address the current issues, but the idea of adopting a new scheme makes the discussants feel insecure because it might upset the strategic balance, or create confusion, so the discussants stick to the old habit. Another motivation can be collective ostrich policy: neither of the discussants wants to face certain aspects of the issue under discussion, since these are felt as inconvenient or otherwise unpleasant. More or less latent power factors can also play a role, giving rise to self-censorship (cf. Mitchell, 2003)**[iv]**, or to implicit effects of an interviewer's questioning as addressed in psychology by Schwarz (1994) under the term 'logic of conversation').

Such collective failures of content can be conceived as failures of explicitisation. Yet, they do not violate the pragma-dialectical rules as formulated by van Eemeren and Grootendorst (1984; see 2003 for a recent version). The reason is that the pragma-dialectical rules focus on fairness. They translate the desirability of explicitisation problem into the right of discussants to bring up anything they choose. In their explanation of the pragma-dialectical rules van Eemeren and Grootendorst wrote:
'So the importance of externalizing disputes is plain, and it therefore follows that one of the most important tasks to be achieved in formulating rules for rational discussion is the furtherance of an optimal externalization of disputes. This means that the discussants must be able to advance every point of view and must be able to cast doubt on every point of view.' (van Eemeren, Grootendorst, 1984: 154)**[v]**

But the discussants having a right does not imply that they will always use it. In as far as their goals are opposed, they probably will; but when they implicitly agree – consciously or unconsciously – not to address certain aspects, explicitization is no longer guaranteed. Freedom of speech may be a necessary condition for explicitization, but it is definitely not a sufficient one. As long as power inequalities are involved, one could still hold that the pragma-dialectical rules are violated because there is no complete freedom – even though it will

sometimes be hard to prove that the failure is involuntary on the part of at least one of the discussants. In many of the cases of level (ii) and (iii) failure discussed earlier, however, power inequality is not the dominant cause.

Finally, it is worthwhile to observe that in some cases the obstacles presented by collective failures as discussed above can be enhanced by differences in framing between the discussants. When the discussants have a different framing of the issue at stake or of certain premises, this may create serious obstacles to mutual understanding (Birrer,Pranger, 1995; Wohlrapp, 1995; Vermaak, 1999). Several of the obstacles discussed above can be viewed as clashes between different framings, such as the different conceptualisations of the notion of privacy, and the distrust paradox. In such framings propositions cannot be understood in isolation, but only as embedded in complex packages, and discussants tend to either accept or reject a whole package. In as far as it is possible at all to work out some common ground, the amount of work required may be very substantial. This problem is even greater when the frameworks stand in polarisation towards each other, like in the case of the distrust paradox.

6. Conclusions

Sometimes discussants collectively refrain from addressing certain aspects that are relevant to the subject of their discussion. Such cases could be said to go against the spirit of a reasonable discussion, and as such also against the spirit that has guided the formulation of the pragma-dialectical rules, but in a formal sense they do not present an infringement of those rules as they have been formulated. It seems important, nevertheless, to identify such collective failures. In order to do this, the analyst may have to go beyond what the discussants themselves bring forward, and may have to try to answer the question what exactly the discussants would have been discussing if no main relevant aspects had been suppressed.

NOTES

[i] Technical introductions in the field of data mining can be found in (Witten, Frank, 2000), and (Hand, Mannila, Smyth, 2001).

[ii] Similar arguments can be found in a wide variety of other contributions to the debate, such as Safire’s (2002) column, the comprehensive juridical analysis by Taipale (2003) or the statements by the American Civil Liberties Union (ACLU, 2003).

[iii] The interpretation of the Fourth Amendment, however, is prone to

ambiguities as well. Braverman and Ortiz (2002) observe a tension between the first part refering to “unreasonable searches” and the second part refering to “probable cause”, the first allowing considerable more discretion than the second. An illustrative example of confusion concerning the Fourth Amendment occurred at a press conference by General Hayden on January 26, 2006. He was interpreted by many as denying that the Fourth Amendement refered to probable cause at all (which would be obviously incorrect). See White (2006) for a defense of Hayden, arguing that Hayden was talking about the first clause involving “unreasonable searches”, and that the “probable cause” mentioned in the second clause applies to warrants for search, and not directly to the first clause as such. Since that distinction was not explicitly made by Hayden, however, a less charitable interpretation, and one in fact picked up by many, would be that Hayden was unaware that the Fourth Amendment mentioned probable cause.

[iv] Illustrative for the complications of issues of self-censorship is the recent debate in the US on the question whether newspapers should reveal ‘security’ information. The controversy could already be sensed when James Risen and Erich Lichtblau in the New York Times reported secret eavesdropping by the National Security Agency (Risen, Lichtblau, 2005), and two days later President Bush in a radio speech stated (without explicit reference to the New York Times) that ‘Revealing classified information is illegal, alerts our enemies, and endangers our country.’ (Bush, 2005). In 2006 a more extensive public debate arose when the press made public that the CIA has access to European Swift bank transfer data (Lichtblau, Risen, 2006; Baquet, Keller, 2006).

[v] Their views apparently have not changed in the meantime, in 2003 they wrote quite similarly:

‘The importance of the externalization of differences of opinion is therefore evident. One of the first tasks in the formulation of rules for a critical discussion is thus to promote an optimal externalization. This means that the discussants must be able to put forward every standpoint and to call every standpoint into question.’ (van Eemeren, Grootendorst, 2003b: 366)

Perhaps these ideas can be traced to the article by Grice (1975) that was an important starting point for van Eemeren and Grootendorst. Grice’s analysis is based on the idea of conversation as a cooperative endeavour, solving a common problem defined by common goals. This leaves it entirely to the participants to (implicitly or explicitly) decide what the common goals are, rather than submitting these goals to an external evaluation. Similar remarks can be made regarding the five ‘language rules’ derived by van Eemeren and Grootendorst

from their Communication Principle (in turn inspired by Grice's Principle of Co-operation): the second principle demands 'sincerity' and 'honesty' of the discussants (see van Eemeren, Grootendorst, 2003a: 77), which prima facie seems to imply full externalisation, but again the resulting rules for critical discussion do not exclude collective failures of the kind discussed above.

REFERENCES

ACLU (American Civil Liberties Union) (2003) *Total information compliance: The TIA's burden under the Wyden Amendment. A preemptive analysis of the government's proposed super surveillance program*, May 19, 2003.

Alexander, Y (2001). *Terrorism: a definitional focus. In: Terrorism and the law* (Y. Alexander, E.H. Brenner), Ardsley (NY): Transnational Publishers.

Baquet, D, & B. Keller (2006). When do we publish a secret?, *New York Times*, July 1, 2006

Birrer, F.A.J., & M.A. Mentzel (2005). *Issues of power, risk and ethics in the biotech debate, LIACS Technical Report 2005-09*, Leiden University.

Birrer, F.A.J. (2004). Subliminal enticement and the ethics of sustainable agricultural production. In: J. de Tavernier, S. Aerts (eds.), *Science, ethics & society* (EURSAFE 2004), Leuven: Katholieke Universiteit Leuven, pp. 190-193.

Birrer, F.A.J. (2001a). Expert advice and argumentation, *Argumentation* 15, 267-275.

Birrer, F.A.J. (2001b). Applying ethical and moral concepts and theories to IT contexts: some key problems and challenges. In: R.A. Spinello, H.T. Tavani (eds.), *Readings in cyberethics* , Sudbury (MA): Jones & Bartlett Computer Science, pp. 91-97.

Birrer, F.A.J., & R. Pranger (1995). Complex intertwinements in argumentation. In: F.H. van Eemeren, R. Grootendorst, J.A. Blair, C.A. Willard (eds.), *Proceedings of the Third ISSA conference, 1995, International Centre for the Study of Argumentation,* Amsterdam.

Bush, G.W. (2005). *President's radio address*, December 17.

Coleman, Jr., W.T. (2004). *Separate statement of William T. Coleman,* in (TAPAC, 2004).

DARPA (Defense Advanced Research Projects Agency) (2003). *Report to Congress regarding the Terrorist Information Awareness Program* (in response to Consolidated Appropriations Resolution, 2003, Pub. L. No. 108-7, Division M, § 111 (b)), May 20, 2003, DARPA.

Doyle, C. (2006). *Memorandum to the Senate Select Committee on Intelligence*,

January 30, 2006, Washington.
Eemeren, F.H. van, & R. Grootendorst (2003a). *A systematic theory of argumentation*, Cambridge: Cambridge University Press.
Eemeren, F.H. van & R. Grootendorst (2003b). A pragma-dialectical procedure for a critical discussion, *Argumentation* 17, 365-386.
Eemeren, F.H. van, & R. Grootendorst (1984). *Speech acts in argumentative discussions. A theoretical model for the analysis of discussions directed towards solving conflicts of opinion*, Foris: Dordrecht.
GAO (General Accounting Office) (2004). Data mining. Federal efforts cover a wide range of uses. *GAO Report* 04-548, Washington, D.C.: GAO.
Govier, T. (1987). *Problems in argument analysis and evaluation*, Dordrecht/Providence: Foris.
Grice, H.P. (1975). Logic and conversation. In: D. Davidson, G. Harman (eds.), *The logic of grammar, Encino* (CA): Dickenson Publishing Company.
Hand, D., & H. Mannila & P. Smyth (2001). *Principles of data mining*. Cambridge (Mass.): MIT Press.
Lichtblau, E., & J. Risen (2005). *Bush lets U.S. spy on callers without courts*, New York Times, December 16.
Lichtblau, E., & J. Risen (2006). Bank data is sifted by U.S. in secret to block terror, *New York Times*.
Mena, J. (2004). *Homeland security. Techniques and technologies*. Hingham (Mass.): Charles River Media.
Mitchell, G.R. (2003) American itsesensuuri: a typology of self-censorship in the 'War on terror', in F. H. van Eemeren, A. Blair, C. A. Willard, A. F. Snoeck Henkemans (eds.), *Proceedings of the Fifth Conference of the International Society for the Study of Argumentation*, Amsterdam: SicSat, pp. 767-772.
Office of the Inspector General, Department of Defense (2003). *Information technology management: terrorism information Awareness program* (D-2004-033), December 2003, Department of Defense.
Safire, W. (2002). You are a suspect. *New York Times*. November 14, 2002, p. A 35.
Schwarz, N. (1994). Judgment in social context: biases, shortcomings, and the logic of conversation. In: M.P. Zanna (ed.), *Advances in Experimental Social Psychology*, vol. 26, San Diego: Academic Press.
Taipale, K.A. (2003). Data mining and domestic security: connecting the dots to make sense of data. Columbia Science and Technology Law Review 5 (2) 1-83.
TAPAC (Technology and Privacy Advisory Committee) (2004). *Safeguarding*

privacy in the fight against terrorism. March 2004, Washington, D.C.: Department of Defense.
U.S. Supreme Court (1976). *United States v. Miller*, 425 U.S. 435.
Vermaak, M. (1999). On conversational constraint. In: F.H. van Eemeren, R. Grootendorst, J.A. Blair, A. Willard (eds.), *Proceedings of the Fourth International Conference of the International Society for the Study of Argumentation*, Amsterdam: SicSat, pp. 829-832.
White, A. (2006). Unwarranted criticism. General Hayden's reading of the Fourth Amendment is correct, and his critics are mistaken. *National Review*, May 10, 2006.
Whittaker, D.J. (ed.) (2001). *The terrorism reader*. London: Routledge.
Witten, I.A., & E. Frank (2000). *Data mining.* San Francisco: Morgan Kaufmann.
Wohlrapp, H. (1995). Resolving the riddle of the non-deductive argumentation schemes. In: F.H. van Eemeren, R. Grootendorst, J.A. Blair, C.A. Willard (eds.), *Proceedings of the Third ISSA conference*, Vol. 2, Amsterdam: International Centre for the Study of Argumentation, pp. 43-57.