

## Could Do Better? – Hegemony and Freedom in Cyberspace

Several commentators have commented on the apparent ‘irony’ of Google’s resolute determination on the one hand to resist the demands by the USA’s Department of Justice (DoJ) to divulge millions of search records and its willingness on the other to self-censor voluntarily its Chinese search engine in deference to the central authorities in that country. The cry of hypocrisy is easily made. But is it fair or, indeed, reasonably informed? Certainly the issues surrounding censorship and freedom of information are not always as straightforward as popularly imagined.

Google’s corporate motto “Don’t be evil” may at first sight seem high-minded, bordering on the theological, but is perhaps better, if less exotically, located in the idea of *nonmaleficence*. The latter certainly finds a welcome home in the deontological ethics of W.D. Ross which sought to relate *prima facie* duties to actual moral convictions in specific circumstances .

Google’s apparent lack of consistency in its respective dealings with the DoJ and the Chinese authorities is itself complicated by its own corporate ambitions. The spectacular success of Google as a search engine has been well documented. Its pole market position, relative to Yahoo, MSN Search, Altavista, Jeeves and others, is already well established and likely to be enhanced by such diversifications as Gmail, Google Earth, Picasa and Book Search. This does not necessarily mean that there cannot be room for niche search engines or that a rival company is in any way constrained in developing a fundamentally different (i.e. more intelligent or intuitive) search engine in the future. Nonetheless the future does look bright for Google as it has, like Microsoft, effectively cornered the market – at least for the foreseeable future. Moreover technology is on its side with the inexorable advancement of higher capacity, and also cheaper, data storage, along with greater communication bandwidth.

Google’s stated mission is “to organize the world’s information and make it universally accessible and useful”. At first sight such a statement seems remarkably benign. However we need to be mindful of the fact that privacy has in the past been secured not such much by legal entitlement, but rather by the relative *disorganisation* of information. It is difficult to gainsay that the gathering and indexation of data on a global basis poses real and substantial threats to personal privacy. Why should we feel less anxious about hegemonistic approaches to knowledge (as understood, say, in Poppers ‘World 3’ sense) by large corporations than we would by national governments or perhaps international institutions?

The retention of personal data has profound implications. Notwithstanding substantial lobbying by civil society groups, including the European Digital Rights Campaign (EDRI), the EU Data Retention Directive, for example, was adopted by the European Parliament in December 2005. In February 2006 it was adopted by the Ministers of Justice and Home Affairs Council (JHA) – despite outright opposition by Irish and Slovakian representatives as well as substantial parliamentary misgivings in the Netherlands and Finland. In short the Directive requires all member states within the EU to introduce *mandatory* data retention for telephony and internet data, for a period between 6 to 24 months. Perhaps more significant is the fact that the directive is not limited to the ‘fight against terrorism’ and organised crime, but now embraces all serious crimes as defined by each individual member state. A few months earlier, the Report of the Tunis phase of the World Summit on the Information Society (WSIS) spoke about creating a “global culture of cybersecurity”. Such a culture, according to WSIS, “requires national action and increased international cooperation to strengthen security *while enhancing the protection of personal information, privacy and data* [my italics].” It is not clear how the EU Data Retention

Directive can be seen as taking to heart WSIS's desire for countries to take a principled approach in this particular area.

Google's resistance against the US government's subpoena had several strands. However, it is important to note in the first instance the specific context of the subpoena, namely the determination of DoJ to effect the Children's Online Protection Act (COPA) passed by Congress in 1998. In particular DoJ was anxious to demonstrate that filtering technology was not effective in preventing children from reaching pornographic sites. Originally the DoJ requested all major ISPs and search engines to submit "all queries that have been entered into your company's search engine between June 1, 2005 and July 31, 2005". Following resistance, it agreed to a more limited request that included a random sample of one million web addresses together with a list of every search string during a one-week period. In January 2006, Yahoo, AOL and Microsoft indicated that they would comply with DoJ's modified request. Google, however, decided that it ought to continue to resist the subpoena robustly on the basis that even the modified request raised sensitive issues concerning privilege, privacy and proprietary rights that would render compliance both unreasonable and oppressive. In March the case was heard by District Judge James Ware who ordered Google to turn over a much smaller sample of search data – limited to 50,000 web addresses and 5,000 search terms – to the US government. According to Nicole Wong, an associate general counsel for Google, the ruling sends a clear message about privacy insofar as it indicates "that neither the government nor anyone else has *carte blanche* when demanding data from internet companies".

In contrast, Google's full compliance with the request or wishes of the Chinese authorities means that it is now willing to block politically sensitive terms on its new China search site – Google.cn – and not provide e-mail, chat or blog publishing services as elsewhere. Previously it had only censored its news site in China by removing banned material, but had not taken the more draconian measures of its competitors of actually censoring its US-based search engine. According to co-founder Sergey Brin: "The practical matter is that over the last couple of years Google was censored – not by us but by the government, via the 'the Great Firewall'...France and Germany require censorship for Nazi sites, and the U.S. requires censorship based on the Digital Millennium Act. These various countries also have laws on child pornography". Such a policy shift, though essentially pragmatic, has inevitably attracted the ire of media libertarians. Reporters Without Borders, for example, contends that company's new policy is immoral and unjustifiable. In a statement it argues that "by offering a version without 'subversive' content, Google is making it easier for Chinese officials to filter the Internet themselves. A Web site not listed by search engines has little chance of being found by users...The new Google version means that even if a human rights publication is not blocked by local firewalls, it has no chance of being read in China".

Some claim, and with considerable passion, that the Internet (which must not be equated *tout simple* with the World Wide Web) should remain an unlimited playground for the free exchange of ideas and information, an ideologically ramshackle world beyond hierarchical control. Notwithstanding the phenomenal rise of blogging, the Internet has become in recent years not so much a playground but rather a weary battleground in which ideologues and those with obvious vested interests seek practical influence and domination. The truth is that the Net not merely *reflects* certain social or geo-political realities but is now itself an extraordinarily powerful *instrument* in their actual constitution; in this sense the medium remains the message.

Clearly a case can be made for the Justice Department's subpoena in its determination to honour the intentions of Congress in passing COPA. Clearly a case can be made on behalf of the Chinese authorities who fear that the rapid adoption of western-style forms of democracy

might derail the country's current economic advance. Clearly a case can also be made for Google's desire to offer the public the most comprehensive and advanced approach to data gathering and indexation. However, in each instance, we are left with a profound, almost eerie, sense of unease.

The right to privacy and the right to information are more finely balanced than we frequently think. Neither child protection policies nor anti-terrorist strategies should become an alibi for defending any panoptical *folie de grandeur* on the part of the State. Nor should the prospect of economic prosperity smother the concerns of those who wish to think or live 'differently' within society. Human rights language may have its problems, but the moral convictions to which it persistently refers are more often than not rooted in genuine human predicaments which require either redress or, at least, ameliorative action. Finally, neither technical ability nor commercial viability is an adequate substitute for proper moral debate when it comes to considering the collection, ownership and distribution of data. The *summum bonum* of the Internet ultimately rests on the responsibility of all its participants to ask the critical question '*Cui bono?*' repeatedly when it comes to the collection, manipulation and maintenance of personal data.

---

Ian Kenway is Director of the Centre for the International Study of Cyberethics and Human Rights ([CISCHR](#)) and Honorary Research Fellow in Ethics and ICT at Cardiff University.