6a

Some recent challenges to openness and freedom in scientific publication

David B. Resnik[#]

"The right to search for truth implies also a duty; one must not conceal any part of what one has recognized to be true."
Albert Einstein, engraved on his memorial statue at the National Academy of Sciences, Washington, DC.

Introduction

Most scientists probably share Einstein's commitment to searching for and revealing the truth. This commitment implies a variety of ethical norms and values, including honesty, integrity, objectivity, openness, freedom, carefulness and fairness (Shamoo and Resnik 2002). However, professional ambitions and rivalries, financial interests, intellectual property disputes, ideological agendas and other social, economic and political influences can disrupt or derail the quest for the truth (Ziman 2002; Kitcher 2001). Since modern research is a social phenomenon, it is not possible to eliminate these social, economic and political factors from the scientific milieu (Kuhn 1970; Hull 1988; Longino 1990). Even so, scientists, research sponsors and academic institutions should strive to maintain a strong commitment to the search for the truth, and they should develop policies and institutions that minimize the impact of external biases and influences on research (Shamoo and Resnik 2002).

Many of the important ethical problems and issues in scientific research reflect the clash between science's ethical ideals and these non-scientific (external) influences in the contemporary research environment (Resnik 1998). Nowhere has the clash between scientific and non-scientific values been more evident than in the area of publication and the dissemination of information, where private and government interests may conflict the scientific commitment to search for and reveal the truth. This paper will discuss several recent problems for openness and freedom in scientific publication related to the private sponsorship of research and the threat of bioterrorism. The paper will also suggest some potential solutions to these problems.

Private industry and the suppression of research

Private industry sponsors more than half of all research and development (R&D) conducted in the world. In the year 2000, private industry accounted for roughly 60% of the $200 billion that the United States (US) spent on R&D (Shamoo and Resnik 2002). Private investment in R&D, which had been less than the public investment in R&D throughout the 1960s and 1970s, rose significantly in the 1980s and 1990s,

[#] Brody School of Medicine, East Carolina University, 2S-17 Brody Building, Greenville, N.C., 27858, USA. E-mail: resnikd@mail.ecu.edu

while public investment rose only marginally. Most of the increase in private R&D was due to the continued growth of the pharmaceutical industry and the emergence of the computer and biotechnology industries. Since businesses have strong economic motives to invest in R&D and government budgets constrain increases in public investment in R&D, it is likely that the private sector will outspend the public sector for many years to come.

The infusion of private money into science has benefited researchers, businesses, universities and society, but it has also taken a toll on openness and freedom in research. Businesses aim to make a profit and to produce goods and services. They do not search for the truth for its own sake; they regard R&D as a necessary means of achieving financial and practical goals, and they are more than willing to restrict openness or freedom in order advance their primary goals.

If a scientist is employed by a private company to conduct research, the company will usually make him sign a contract in which he agrees that the company owns all of his data and has the authority to review and approve any of his publications. Even a scientist employed by a University may sign a contract with a private company that sponsors his research, which gives the company the right to review his research and approve of any publications. Although some universities do not allow their employees to sign these contracts, many do. A scientist who violates the provision of one these contracts can face adverse legal consequences, including civil liability for breach of contract or negligence as well as criminal liability for disclosing trade secrets.

There are at least three reasons why a private company would want to prevent a scientist from publishing research sponsored by the company. First, the company might seek to block publication in order to protect its intellectual property rights. Publication of information used to develop a patentable invention may count as a prior disclosure. Patent laws in the US and Europe require that the invention be novel. If the invention has already been publicly disclosed, then it will not meet the novelty requirement and it will not be patentable (Miller and Davis 2000). Although patenting can delay publication of scientific and technical information, in the long run it encourages public disclosure because the patent application becomes a part of the public record. Thus, although intellectual property interests can pose a short-term threat to the search for the truth, in the long run they benefit science by providing incentives for inventors, investors and entrepreneurs.

A second reason why a company might want to block research is that it does not want its competitors to discover its new products, business strategies or other trade secrets. It wants to maintain secrecy in order to secure a competitive advantage. Although the desire for trade secrecy can inhibit the search for the truth in the short term, in the long run many of the secrets that a company keeps will become public knowledge as the company places goods and services on the market, implements business strategies and discloses its secrets. Other secrets may be discovered by legal means, such as reverse engineering or independent research (Shamoo and Resnik 2002). A more troubling reason why a company might want to block publication is that publication of adverse data or results may undermine its ability to market a particular good or service. For example, if a company sponsors research that compares its drug to competing drugs, and the research demonstrates that its drug is no better than the competitors', it might try to suppress publication of the research. Or even worse, if a company sponsors a study that shows that its product is dangerous, it might try to suppress this research as well. Three highly publicized cases have illustrated problems with the suppression of research.

In 1994, the US Congress held hearings on the tobacco industry. A Congressional committee subpoenaed the testimony of Drs. Victor DeNobel and Paul Mele, who conducted research for Philip Morris on nicotine addiction in the 1980s. DeNobel and Mele testified that their research proved that nicotine is highly addictive and that they discovered substances that increase the addictive properties of cigarettes, while reducing the adverse cardiovascular effects of cigarettes. The purpose of their research was to develop a substitute for nicotine that would make cigarettes more addictive. DeNobel and Mele, who were employees of Philip Morris, were not allowed to discuss their work with other employees or colleagues. Animals used in their research were brought into the laboratory under covers. The two scientists tried to publish the results of their work in *Psychopharmacology*, but Philip Morris learned about the paper and forced DeNobel and Mele to withdraw their paper. The company also dismissed the two scientists and shut down their laboratory. DeNobel and Mele had signed a contract with Philip Morris in which they agreed never to discuss their research without the company's permission, but Congressman Henry Waxman arranged for the two scientists to be released from this agreement so they could testify before Congress (Hilts 1994).

In 1995, the Boots Company made Dr. Betty Dong withdraw a paper on drugs used to treat hypothyroidism, which had been accepted by the Journal of the American Medical Association. Boots had funded Dong's research, which compared its drug, Synthroid, to some generic drugs. Boots found that Synthroid was not safer or more effective than the generic drugs and that the US could save millions of dollars a year if patients switched from Synthroid to one of the generic drugs. Dong, who was a clinical pharmacologist at the University of California at San Francisco, had signed a contract with Boots giving the company permission to review her results and prevent her from publishing her work, without written permission. The company threatened to sue Dong and also spent two years attempting to discredit her research. To avoid a lawsuit, Dong withdrew the paper. However, the company eventually relented, and two years laters Dong published her results in the *New England Journal of Medicine* (Wadman 1996; Shamoo and Resnik 2002).

From 1993 to 1995, Dr. Nancy Olivieri and her colleagues at the University of Toronto and Toronto General Hospital conducted research on a drug used to treat thalassaemia, deferiprone. Their research was sponsored by Apotex Inc., a Canadian pharmaceutical company. In 1995, Olivieri and her collaborators published an article on deferiprone in the *New England Journal of Medicine*. The study reported that the drug was effective at reducing total body iron stores in thalassaemia patients and had manageable side effects. A few months after they reported these positive findings, they observed that liver iron stores in many of their patients were reaching dangerous levels, which could lead to heart failure or death. Olivieri wanted to notify the hospital's Research Ethics Board (REB) about this problem, so that the consent forms could be revised and patients could learn about this new risk. Apotex tried to prevent Dr. Olivieri from reporting her concerns to the REB. She did eventually notify the REB, but after she did, the company terminated the study and withdrew all the supplies of the drug from the hospital pharmacy. The company also threatened to bring litigation against Olivieri if she would decide to tell patients, regulatory agencies or the scientific community about her concerns. Several other studies confirmed Olivieri's concerns about the drug. She continued to receive letters from the company threatening legal action, and she withdrew some presentations on the drug she had planned to make at scientific meetings (Olivieri 2003).

In 1998, Apotex, which was negotiating a large donation to the University and the Hospital, pressured these institutions to take actions against Olivieri. Olivieri had assumed that the Hospital and the University would take her side in the dispute with Apotex, but these two institutions denied there was a problem, sought to delay public awareness of the problem, tried to divide Olivieri from her colleagues, sought to discredit her work, and even tried to have her dismissed from her position. Finally, in January 1999, an international group of ethicists and scientists lent their support to Olivieri and prevented her from being dismissed. Olivieri reached an agreement with the Hospital and the University, clearing her of all allegations. In 2000-2001, a commission from the Canadian Association of University Teachers investigated the incident (Olivieri 2003).

Clearly, the suppression of research by private industry represents a significant threat to the search for the truth, since a private company could use this strategy to the published research record, to keep undesirable results a secret or to control the conduct of scientists. How should the scientific community respond to this problem? Private companies should be encouraged to sponsor R & D, provided that they adhere to some rules for publication. To develop these rules, we should distinguish between different types of research: industry-sponsored research conducted in a university (or academic) setting and industry-sponsored research conducted in private laboratories. Since openness and freedom are vital to the academic environment and university-based research, universities should not allow their faculty to sign contracts that grant private companies the right to block the publication of research conducted on campus. No private company should be able to suppress academic research. All contracts signed by academic researchers with private companies should give them the right to publish data as soon as it is necessary to promote the advancement of research or address important public-health or safety concerns. Additionally, academic institutions should support researchers who become involved in disputes with private companies about publishing data and results (Nathan and Weatherall 2002).

What about research conducted in private laboratories? Should governments enact laws that forbid private companies from signing employees to contracts granting the company the right to suppress publication of research conducted for the company?

Although it would be desirable to encourage private companies to guarantee the same degree of freedom and openness that one finds (or expects to find) in academia, restrictions on the contracts that private companies sign with their employees would be unwise. First, in the US (and possibly in other countries), such restrictions would run into legal challenges. In the US, laws that restrict the freedom of private contracts must have a reasonable relationship to the public interest, and they should be neither arbitrary nor discriminatory (Nebbia v. New York 1934). Private companies that sponsor research could argue that laws that restrict the contracts they sign with scientists would not serve the public interest because they would discourage companies from conducting research. Second, one might argue that a private laboratory is not the same as an academic institution, because private corporations, unlike academic institutions, are established in order to make a profit. Although academic institutions thrive on freedom and openness, control and secrecy are essential to private businesses. Businesses need to maintain trade secrets to build and maintain competitive advantages. Since trade secrecy should still protect private research conducted in private laboratories, it would be unwise to require businesses to sign researchers to contracts that could undermine trade secrecy. Thus, the research the DeNobel and Mele did for Philip Morris is fundamentally different from the research that Dong and Olivieri conducted for pharmaceutical companies. In both instances, private money supported the research, but in the second instance, the research was conducted in an academic environment. Only in this second instance should there be limitations on private contracts with researchers that are designed to promote freedom and openness.

Private industry and access to data from published research

Another important issue where private industry poses a threat to the search for the truth concerns access to data after publication. Several surveys have shown that many scientists working in academic and non-academic setting frequently refuse to share data prior to publication (Blumenthal et al. 1997; Campbell et al. 2002). The main reasons mentioned by respondents to the survey are that they withheld data in order to protect unpublished work, to secure priority, to protect intellectual property rights, or because data-sharing was inconvenient or expensive. These are all good reasons to guard data prior to publication. First, prior to publication, data may be inconclusive or unconfirmed. Premature publication of data or results can have disastrous effects, as illustrated by the cold-fusion controversy (Shamoo and Resnik 2002). In this case, Drs. Stanley Pons and Martin Fleischmann believed that they had discovered a way to produce fusion at room temperature in an electrolytic solution. Pons and Fleischmann presented incomplete descriptions of their methods as results at a press conference before submitting their work for peer review. Scientists around the world scrambled to try to replicate their results, but they were unsuccessful. Many scientists were upset that Pons and Fleischmann published their data through a press conference prior to peer review; other accused them of fraud, negligence or self-deception. The entire episode had a negative impact on the public's perception of science.

Second, important claims to intellectual priority may be at stake when scientists are asked to share unpublished data. Priority disputes have occurred in science for hundreds of years. In science, the credit goes to the researchers who publish first (Merton and Storer 1973). If a researcher shares his or her data with someone else before it is published, he or she may not receive credit for making an important discovery, and the person that received the data might steal the researcher's work and take credit for the discovery. Priority is also important in establishing patent rights. To be patentable, an invention must be novel, non-obvious and useful. An invention that has been previously disclosed through prior publication or use will not be considered novel (Miller and Davis 2000). A researcher who shares or publishes data before filing a patent application may lose his or her legal right to patent the invention. Furthermore, someone else could use shared data to beat the researcher in the race for patent rights. If two researchers both apply for a patent on the same invention, patent offices will award the patent to the first person to conceive of the inception, provided that they have both exhibited due diligence in prosecuting the patent application and reducing the invention to practice (Miller and Davis 2000).

Although researchers often have good reasons not to share data prior to publication, they should share data after publication, if sharing data will not violate the privacy of research subjects. Once a researcher has published the results of his scientific work and received proper credit for his or her accomplishments, he or she should make his or her data available to other researchers. It is important to share data after publication because other researchers may need the data to verify the results, repeat the experiments, to learn how the research was conducted or to stimulate new discoveries and findings (Shamoo and Resnik 2002). In the US, government agencies that sponsor research, such as the National Institutes of Health (NIH), require researchers who receive contracts or grants to share data once the main results of a research project have been accepted for publication (National Institutes of Health 2003). However, these data-sharing rules do not apply to private corporations, which may decide to publish the results of a research project and then charge a fee for access to the data. Even though many scientists share data after publication, some still refuse to share data after publication. One reason why researchers may not share data supporting published results is that one may still make important discoveries by analysing the unpublished data, and some scientists do not want researchers who have not invested time, money and effort in gathering data to take undeserved credit for publications based on the data (Barinaga 2003). Another reason for not sharing unpublished data is that an individual or a group with a political agenda, such as an animal-rights group, could use the unpublished data to harass the researcher.

In February 2001, the public consortium, led by the National Human Genome Research Institute (NHGRI), and Celera Genomics, a private company, published versions of the human genome in the journals *Nature* and *Science*, respectively. The NHGRI deposited its data relating to the human genome in the Genbank, an enormous electronic database that researchers can access for free. Celera, however, refused to deposit its data in the Genbank. Under the terms and conditions negotiated between *Science* and Celera, non-profit researchers were allowed to download data from Celera's website, provided that they agreed not to commercialize or distribute the data. Researchers who planned to use the data for commercial purposes were required to negotiate an agreement with Celera (Marshall 2001). *Science* reached a similar agreement with Syngenta when it published a draft sequence of the rice genome (Marshall 2003).

Many scientists were angry that *Science* decided to publish Celera's paper describing the human genome without requiring the company to make its data freely available. In 2003, a group of leading researchers from the biosciences issued a report on sharing data in the life sciences (National Research Council NRC 2003). The report prescribes rules for sharing data and materials known by the acronym UPSIDE (Universal Principal of Sharing Integral Data Expeditiously). The UPSIDE rules recommend that all scientists who publish research on genome sequences should immediately deposit their entire data set in a public database, such as Genbank. The report also declares that scientists should also share materials pertinent to their research findings and explain how they were obtained. The editors of *Science* and *Nature* have both said that they would abide by the UPSIDE rules. When Celera published its version of the human genome, there were no generally accepted rules for data-sharing following publication. Currently, 45% of journals surveyed do not have a data-sharing policy (Marshall 2003).

Placing restrictions on access to published data also poses a significant threat to openness and free inquiry. Ideally, researchers should make all of their data available as soon as they publish their work. In an ideal world, all data would be freely available to all researchers after publication. But, we do not live in an ideal world. In the real world, someone must pay a great deal of money to produce research data and develop and maintain databases. In the real world, governments cannot afford to fund all research and development (R&D), and researchers must draw on private funding. When private companies invest in R&D, they expect to obtain a reasonable return on the investment. If they cannot expect a reasonable return on their investment, then they will stop sponsoring R&D or they use trade secrecy to protect data and results. Neither of these possibilities bode well for the advancement of science, technology or industry. Over the years, private companies that invest in R&D have used a variety of business strategies to gain a return on their investments, including patenting new inventions, copyrighting original works and selling products and services. In the today's research environment, access to electronic databases plays a crucial role in research and development in biomedicine and biotechnology. As a result of advances in bioinformatics, researchers can use computer programs to search and analyse databases in order to discover patterns and connections (Mauer and Scotchmer 1999; Freno 2001). For example, one can use computer programs to compare a mouse DNA sequence to a human DNA sequence or to determine the relationship between a viral DNA sequence and its protein product. The ability to search and analyse data therefore also has a great deal of economic value in research, since scientists may be willing to pay a considerable sum for access to data and the ability to search and analyse databases. Some private companies, such as Celera, have developed business models for selling information services. When Celera published its version of the human genome, it was planning to charge researchers a fee for the ability to access, search and analyse DNA-sequence data (Marshall 2001).

Let's assume that private companies should be able to obtain a reasonable return on the R&D investments, including their investments in developing and maintaining databases. Given this assumption, we need to ask *how* companies should be able to make money from their investments. Let us also assume that companies should be allowed to make money in the traditional ways, i.e., through patents and copyrights and selling their goods and services. Our question then becomes: should companies be able to make money by selling data services? The key to resolving this issue is to find a fair balance between scientists' interests in access to research data/results and private interest in making money from selling access to data/results. Someone must pay for the initial R&D required to generate the data and the subsequent R&D needed to develop and maintain the database. But who should pay?

For a useful analogy, consider scientific journals. Journals have several options for generating income including drawing income from authors (e.g. pages charges), from users (e.g. subscription fees), from advertising, or from institutional sponsors (e.g. government or private corporations). Most journals draw income from all of the different sources, and very few journals do not charge users a fee for access to articles. Those that do not charge a fee to users usually have a great deal of institutional support. In addition, nearly every journal provides some information for free via public databases of abstracts and keywords. For instance, anyone can search MEDLINE for abstracts of articles on prostate cancer, but to get a copy of the full article, one must pay the journal, copy the article in the library or write the corresponding author. Under this system, there are two tiers of sharing. The first tier offers free access to abstracts, which usually contain information about the significant findings and results. The second tier offers access to full articles, which are usually not free.

A two-tier system for research data might work as follows. The first tier would provide raw data to the public, free of charge. The second tier would provide access to data that have been analysed and embellished. Companies could charge a fee for access to the second tier of data and require users to sign a licensing agreement. The first tier would provide researchers with the information they need to confirm published results, but it would not provide researchers with the extra features that can stimulate new research and innovation. The second tier would have economic value because it would be useful to researchers who want to search and analyse databases. For a relevant analogy, consider legal information, such as judicial opinions from legal cases, legislative statutes and materials, and administrative policies and procedures. Most of these materials are available online for free in the US. However, it is not at all easy to find, search or analyse these free materials. Westlaw, a legal-information company, has developed an immense electronic library of legal resources that is easy to search and analyse. Westlaw charges users a considerable fee for access to its private database, even though most of the materials it has are also available for free (somewhere). I would like to suggest that Westlaw provide private companies with a good model for selling information services: companies can make data freely available but also charge a reasonable fee for access to well-organized, searchable and analysed databases. Of course, for the Westlaw model to work, it is also important that companies develop savvy licensing agreements and that governments provide private databases with adequate protection under copyright law (Freno 2001).

The military and classified research

The problems discussed in the previous two sections of this paper arise as a result of the conflict between the values of openness and freedom and the interests of private industry. Problems can also occur when openness and freedom conflict with national and international security interests. For many years, the US military has sponsored classified research related to national and international security, including research on weapons systems, defence systems, reconnaissance devices, intelligence methods, encryption techniques and military strategies and tactics. The phrase 'loose lips sink ships' aptly describes much of the research sponsored by the US Department of Defense (DOD) or conducted at DOD facilities and laboratories (Dickson 1984). Classified research is conducted under strict secrecy rules and is not published or otherwise shared with the public until it is declassified. For example, in 1994 President Clinton declassified thousands of documents pertaining to secret human radiation experiments conducted and sponsored by the DOD from the late 1940s to the 1980s (Moreno 1999). Although the military has been granted the authority to classify research with implications for national and international security, it does not have the authority to classify basic scientific information not related to national security (Atlas 2002).

Disputes concerning the status of basic scientific information related to cryptography have existed since World War II, when the ability to encode and decode messages proved to be very important in the Allies' victory over Germany and Japan. The science of cryptography has made tremendous advances since World War II as a result of the development of computer encryption and decryption programs. Officials from groups concerned with national security, such as the DOD, the National Security Agency (NSA), the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI), have tried to control the public dissemination of cryptography research in order to prevent hostile foreign governments, terrorists groups or criminal organizations from having access to advanced encryption technology. On the other hand, scientific organizations with an interest in the sharing of information as well as private companies with an interest in encryption technologies have attempted to keep basic scientific information out in the open.

The US Congress has passed laws that give the US President the authority to restrict the exportation of technologies to foreign governments if they are likely to aid the development of weapons of mass destruction, support international terrorism, increase the possibility of conflict or prejudice arms-control efforts (Ackerman 1998). However, practical and legal obstacles may prevent the President from effectively using these laws to stop the dissemination of encryption information. From a practical point of view, it is almost impossible to stop the exportation of encryption technology, since computer source codes are very easy to transmit electronically. From a legal point of view, a ban on exports of encryption programs could be an unconstitutional interference with the freedom of speech. During the 1990s, Congress considered several bills that would have given the government a way to decrypt all encrypted messages. The idea was to require that all encryption devices or algorithms contain key-recover techniques, which would allow someone with the right information, i.e. a key-recovery agent, to decrypt the encrypted message. Congress also considered several bills that would make key recovery voluntary rather than mandatory. Civil-rights groups, privacy groups, business groups and computer-science organizations opposed key-recovery legislation. The National Research Council raised some issues relating to the security threats posed by key recovery technology. For instance, what would happen if the wrong person got access to a recovery key? So far, the US and Europeans countries have not adopted key-recovery legislation, although they have attempted to control exports of encryption technology (Ackerman 1998).

Bioterrorism is a relatively recent threat to national and international security. Although governments have developed biological and chemical weapons for many years, in the 1990s military and political leaders, biologists, political scientists, public-health experts and security analysts became increasingly concerned about the possible use of biological or chemical weapons by terrorists on civilian populations. The horrors of the large-scale use of mustard gas during World War I led to the adoption of the Geneva Protocol in 1925, which forbids the use of bacteriological and chemical weapons in war. In 1972, dozens of countries signed the 1972 Biological and Toxic Weapons Convention (BTWC), a treaty that prohibits the development or possession of biological weapons. Although many countries, including the US, Russia and China, have signed the BWTC, as many as 17 countries currently possess or are developing biological weapons (Cole 1996). Although Russia claims that it does not have a bio-weapons programme, scientists in the former Soviet Union had an extensive bio-weapons programme that studied the use of anthrax, botulism, the plague, the Ebola virus and the Marburg virus (MacKenzie 1998).

Iraq used chemical weapons during its war with Iran during the 1980s and during its suppression of a Kurdish uprising in 1988. Iraq has acknowledged to United Nations Weapons Inspectors that it had Scud missiles tipped with biological warheads during the 1991 Persian Gulf War (Cole 1996). After that war, weapons inspectors attempted to determine whether Iraq had biological or chemical weapons or was developing them. Iraq denied that it had any of these weapons and kicked out the inspectors in 1998.

Following a series of debates at the United Nations about Iraq's weapons programme, the futility of inspections and the potential use of these weapons by terrorists, the US and the United Kingdom (UK) invaded Iraq in late March of 2003 to enforce UN Security Council Resolution 1441, to find and eliminate these alleged weapons, and to remove Saddam Hussein, the leader of the Iraqi government, from power. (This essay will not engage in a debate about the moral or political justification of this military operation, or lack thereof.) At the time of the writing of this essay, neither the US nor the UK have found any conclusive evidence of biological or chemical weapons in Iraq, but it could take months to conduct a thorough search of the country.

The leaders of the US and UK were concerned that the Iraqi regime might provide chemical, biological or nuclear weapons to terrorist groups, such as Al-Qaeda, the organization which is held responsible for dozens of attacks on civilian targets, including the destruction of the World Trade Center towers on 11 September 2001. Documents and tape-recording from Al-Qaeda indicate that it is interested in acquiring weapons of mass destruction and using them on civilians. Although Al-Qaeda has not used these weapons, on 20 March 1995 the terrorist cult Aum Shinrikyo ('Supreme Truth') released sarin gas in a Tokyo subway, killing 12 people and injuring 5,500. The cult group also attempted, unsuccessfully, to spray anthrax spores over Tokyo (Cole 1996). In the autumn of 2001, someone – the culprit has not been caught – mailed anthrax spores to dozens of people in the Eastern US, killing four victims and sickening 20 others. The anthrax attacks caused a huge panic in the US as thousands of Americans took the antibiotic Cipro as a prophylactic measure. The idea that a terrorist group might one day use biological, chemical or nuclear weapons on civilian or military targets is not a paranoid fantasy; it is a real threat that should be taken seriously (MacKenzie 1998).

Given this social and political background, one can see why publishing information about how to make weapons of mass destruction could pose a significant threat to security. In the past two years there have been at least three papers published in prominent scientific journals that discussed methods and results pertaining to the genetic manipulation of deadly viruses. The papers were published while the US was assessing the threat posed by the use of smallpox as a bio-weapon and considering measures to address this threat, such as instituting a vaccination programme (Bozzette et al. 2003). In February 2001, the *Journal of Virology* published a paper that described the insertion of the gene for interleukin-4, an immune protein, into a mousepox virus. The researchers were trying to develop a method for rendering mice infertile. Instead, they developed a form of the virus that was much deadlier than the naturally occurring strain. The virus even killed mice that had been vaccinated against mousepox (Jackson et al. 2001). In June 2002, *Proceedings of the National Academy of Sciences* published a paper describing an experiment in which scientists formed a new smallpox protein complex, know as smallpox inhibitor of complement enzymes (SPICE), from a virus related to *Orthopoxvirus variola*, the virus that causes smallpox. Since the experiments also showed that the new protein deactivated human immune-system molecules C3b and C4b, a bio-weapon that delivered a genetically engineered smallpox virus with the new protein might be able to infect even people who have received the smallpox vaccine. The paper did mention, however, that it would be important to know how to disable the SPICE proteins (Rosengard et al. 2002). On 9 August 2002 (online version 11 July 2002), the journal *Science* published a paper on the creation of a polio virus by mail-ordering DNA from a private reagent company. The genetically engineered polio virus was capable of paralysing and killing mice (Cello, Paul and Wimmer 2002).

Many politicians and scientists objected to the publication of these papers and called for measures to censor biological research that poses security risks (Couzin 2002).

Several members of the US Congress introduced a resolution criticizing the publication of the polio-virus paper published in *Science*. In January 2003, the American Society for Microbiology (ASM), the National Academy of Sciences and the Center for Strategic and International Studies held a meeting in Washington, DC to discuss the censorship on biological research that poses security risks (Malakoff 2003). At the meeting, the editors of *Science, Nature* and a dozen other major journals said that they were already scrutinizing papers that raise security concerns, but that, so far, they had not rejected any. Several people at the meeting urged scientists to develop their own rules for self-censorship before governments start censoring scientific information (Atlas 2002).

This paper will not attempt to solve all of the complex problems concerning openness, freedom and national and international security. However, the paper will make a few general remarks about weapons of mass destruction that may help scientists, political leaders and policy-analysts focus on the important questions. First, there are at least four different ways of controlling the proliferation of weapons of mass destruction: (a) control of materials, (b) control of information, (c) control of scientists, and (d) control of governments or non-governmental groups. For some weapons, controlling the materials used to make the weapons will go a long way to preventing the proliferation. For example, it is difficult to obtain weapons-grade uranium or plutonium to make nuclear weapons. Countries that have signed the Nuclear Non-Proliferation Treaty co-operate with the International Atomic Energy Agency (IAEA) and other non-governmental organizations stopping the proliferation of nuclear weapons (International Atomic Energy Association IAEA 2003). The problem with this strategy is that the materials needed to develop biological or chemical weapons are not very difficult to obtain. Anthrax can be found in rotting carcasses, and most of the chemicals used to make some nerve agents can be purchased as pharmacies, grocery stores and agricultural supply stores.

Information with implications for national or international security is also very difficult to control. After World War II, the US attempted to keep nuclear secrets from the Soviet Union, but the Soviets soon learned how to build the bomb, as a result of their own research efforts and espionage. Today, university physics, chemistry and biology classes provide graduate students with enough information to build chemical, nuclear or biological weapons, and much of this general information is also available for free over the Internet. Indeed, the Internet has created tremendous challenges for controlling the flow of information by making it much easier to publish scientific information. Several decades ago, a handful of journals, government agencies and publishers would have been able to control most of the information related to constructing weapons of mass destruction. Today, almost anyone with a computer and a connection to the Internet can publish this information.

It may be somewhat easier to control scientists than it is to control materials or information. No country or terrorist group can develop weapons of mass destruction without the assistance of highly skilled scientists. After the fall of Saddam Hussein's regime, it will be very important to locate Iraqi scientists who may have been involved in Iraq's weapons programmes and employ them in peaceful activities. Although scientists are also difficult to control, it is certainly possible to influence scientists through employment opportunities, education and training in professionalism and ethics, and peer pressure.

Finally, it may also be possible to exert some control over the governments or non-governmental groups that want to develop weapons of mass destruction. Peaceful nations can exert economic, political and, if necessary, military pressure on countries that are seeking to develop weapons of mass destruction. Countries can also sign and monitor non-proliferation treaties. Although Iraq appears to have resisted a great deal of international pressure to relinquish its weapons programme, other countries, such as South Africa, have capitulated. Non-governmental groups are more difficult to control than governmental groups – how could one seriously negotiate with a terrorist organization such as Al Qaeda? – but it is also possible to exert some influence on these groups as well. For example, the Irish Republican Army, closely associated with the political organization Sinn Fein, agreed to cease its terrorist activities on 19 July

1997, after years of conflict and negotiation. One can also exert some influence or control over countries that sponsor or harbour terrorist groups, such as Afghanistan, which the US invaded, or Syria, which the US has recently criticized for its role in supporting terrorist groups such as Hezbollah.

The upshot of this discussion is that censoring scientific information is probably not a very effective way of preventing weapons or dangerous devices from entering the wrong hands. The most effective strategy is to control access to materials. When this strategy cannot work, it is far more effective to exert some influence over scientists, governments or non-governmental groups than it is to try to control the flow of information. On the other hand, one can acknowledge this conclusion and still maintain that stopping the flow of information to terrorist groups or rogue nations should be one part of a global strategy for curtailing the proliferation of weapons of mass destruction. Although other strategies may be more effective than censorship, this is still a useful strategy. Sometimes keeping some information secret for as long as one can is better than not keeping that information secret at all.

If countries decide to pursue censorship as means of stopping the spread of weapons of mass destruction, it is important to distinguish between scientific, self-censorship and governmental forms of censorship. There is an important legal difference between censorship by organizations that are non-governmental (or are not agents of the government) and censorship by the government. Many countries recognize a legal right to free speech. The US Constitution protects freedom of speech (Barron and Dienes 1999). In order for the US government to place restrictions on the content of non-commercial speech, the government must demonstrate that it has a compelling interest unrelated to the restriction of speech and that the method of restricting speech is the least restrictive method (United States v. O'Brien 1968). While national security is a compelling government interest unrelated to the restriction of speech, one might argue that censorship is not the least restrictive means of protecting this interest. For example, perhaps the government could allow publication in a forum with a limited audience. If one applies the strict scrutiny test to the controversial papers published in the last two years, it is not clear whether the US government would have had legal authority to stop publication of those papers. Another important concern in free-speech laws is vagueness and over-breadth: a law must not be so vague that people do not know whether it applies and not so broad that it deters legitimate speech (Barron and Dienes 1999).

If we consider censorship by non-governmental organizations, such as journals or professional associations, they would not have to face the legal challenges that governments would face, but they would still have to wrestle with moral questions. Journals and professional associations have an obligation to promote freedom, openness and other scientific values (Shamoo and Resnik 2002). On the other hand, they also have a moral responsibility to protect society from harm. In deciding how to respond to research with implications for national or international security, an organization must balance these competing values. Journals and professional associations may consider a number of different options, such as: (a) allow complete publication; (b) allow limited publication (e.g., restricted access to some parts of the publication); or (c) not allow publication. In choosing among these basic options, organizations should consider carefully the facts and circumstances of the case as well as the following factors relating to the nature of the security threat: (a) the gravity (or magnitude) of the threat, (b) the probability of the threat, (c) the imminence of the threat, (d) the preventability of the threat, and (e) the scientific and social value of the publication. If the threat posed by an article is grave, probable, imminent and preventable, and the publication has marginal scientific or social value, then a private organization would be justified in taking steps to stop its publication.

It is difficult to say whether any of the three controversial papers mentioned in this essay would meet all five of these conditions. The most dangerous paper was probably the one that described a mutated smallpox protein, because this paper showed people how to make a smallpox virus that might overcome human immunity (Rosengard et al. 2002). On the other hand, this paper could have some redeeming value in that it could help microbiologists and public-health experts learn how to develop immunizations against a smallpox virus that overcomes standard immunities. The irony of restricting dangerous publications is that the same information that could be used to make a deadly weapon could also be used for peaceful and productive goals.

Conclusion

As one can see, private interests and national-security concerns can pose significant problems for openness and freedom in scientific publication. Although this essay has discussed some potential solutions to these problems, more work needs to be done. Since these problems are global in scope, it is incumbent upon the scientists, policy analysts, concerned citizens and political leaders throughout the world to continue to find ways to safeguard openness and freedom in research while responding appropriately to emerging challenges to these values, and to co-operate internationally in the development of policies, practices and procedures.

References

Ackerman, W.M., 1998. Encryption: a 21st century national security dilemma. *International Review of Law, Computers and Technology,* 12 (2), 371-394.

Atlas, R.M., 2002. National security and the biological research community. *Science,* 298 (5594), 753-754.

Barinaga, M., 2003. Still debated, brain image archives are catching on. *Science,* 300 (5616), 43-45.

Barron, J.A. and Dienes, C.T., 1999. *Constitutional law*. 5th edn. West Publishing, St. Paul.

Blumenthal, D., Campbell, E.G., Anderson, M.S., et al., 1997. Withholding research results in academic life sciences: evidence from a national survey of faculty. *JAMA: the Journal of the American Medical Association,* 277 (15), 1224-1228.

Bozzette, S.A., Boer, R., Bhatnagar, V., et al., 2003. A model for a smallpox-vaccination policy. *The New England Journal of Medicine,* 348 (5), 416-425.

Campbell, E.G., Clarridge, B.R., Gokhale, M., et al., 2002. Data withholding in academic genetics: evidence from a national survey. *JAMA: the Journal of the American Medical Association,* 287 (4), 473-480.

Cello, J., Paul, A.V. and Wimmer, E., 2002. Chemical synthesis of poliovirus cDNA: generation of infectious virus in the absence of natural template. *Science,* 297 (5583), 1016-1018.

Cole, L.A., 1996. The specter of biological weapons. *Scientific American,* 275 (6), 61-65.

Couzin, J., 2002. Bioterrorism: a call for restraint on biological data. *Science,* 297 (5582), 749-751.

Dickson, D., 1984. *The new politics of science*. Pantheon Books, New York.
Freno, M., 2001. Database protection: resolving the United States database dilemma with an eye toward international protection. *Cornell International Law Journal,* 34 (1), 165-225.
Hilts, P., 1994. Philip Morris blocked '83 paper showing tobacco is addictive, panel finds. *The New York Times* (April 1 1994).
Hull, D.L., 1988. *Science as a process: an evolutionary account of the social and conceptual development of science*. University of Chicago Press, Chicago.
International Atomic Energy Association IAEA, 2003. *About the IAEA*. Available: [http://www.iaea.org/About/] (1 Apr 2004).
Jackson, R.J., Ramsay, A.J., Christensen, C.D., et al., 2001. Expression of mouse interleukin-4 by a recombinant ectromelia virus suppresses cytolytic lymphocyte responses and overcomes genetic resistance to mousepox. *Journal of Virology,* 75 (3), 1205-1210.
Kitcher, P., 2001. *Science, truth and democracy*. Oxford University Press, Oxford.
Kuhn, T.S., 1970. *The structure of scientific revolutions*. 2nd edn. University of Chicago Press, Chicago.
Longino, H.E., 1990. *Science as social knowledge: values and objectivity in scientific inquiry*. Princeton University Press, Princeton.
MacKenzie, D., 1998. Bioarmageddon. *New Scientist* (Sep 19 1998), 1-8.
Malakoff, D., 2003. Researchers urged to self-censor sensitive data. *Science,* 299 (5605), 321.
Marshall, E., 2001. Sharing the glory, not the credit. *Science,* 291 (5507), 1189-1193.
Marshall, E., 2003. The upside of good behavior: make your data freely available. *Science,* 299 (5609), 990.
Mauer, S.M. and Scotchmer, S., 1999. Database protection: is it broken and should we fix it? *Science,* 284 (5417), 1129-1130.
Merton, R.K. and Storer, N.W., 1973. *The sociology of science: theoretical and empirical investigations*. University of Chicago Press, Chicago.
Miller, A.R. and Davis, M.H., 2000. *Intellectual property: patents, trademarks, and copyright in a nutshell*. West Group, St. Paul.
Moreno, J.D., 1999. *Undue risk: secret experiments on humans*. W.H. Freeman, New York.
Nathan, D.G. and Weatherall, D.J., 2002. Academic freedom in clinical research. *The New England Journal of Medicine,* 347 (17), 1368-1371.
National Institutes of Health, 2003. *Final NIH Statement on sharing research data*. NIH, Bethesda. Notice no. NOT-OD-03-032. [http://grants1.nih.gov/grants/guide/notice-files/NOT-OD-03-032.html]
National Research Council NRC, 2003. *Sharing publication-related data and materials: responsibilities of authorship in the life sciences*. The National Academies Press, Washington DC. [http://books.nap.edu/books/0309088593/html/index.html]
Nebbia v. New York, 1934. 291, U.S., 502 (1934).
Olivieri, N.F., 2003. Patients' health of company profits? The commercialisation of academic research. *Science and Engineering Ethics,* 9 (1), 29-41.
Resnik, D.B., 1998. *The ethics of science: an introduction*. Routledge, London. Philosophical Issues in Science.
Rosengard, A.M., Yu Liu, Zhiping Nie, et al., 2002. Variola virus immune evasion design: expression of a highly efficient inhibitor of human complement.

Proceedings of the National Academy of Sciences of the United States of America, 99, 8808-8813.

Shamoo, A.E. and Resnik, D.B., 2002. *Responsible conduct of research*. Oxford University Press, Oxford.

United States v. O'Brien, 1968. 391 U.S. 367 (1968).

Wadman, M., 1996. Drug company 'suppressed' publication of research. *Nature,* 381 (6577), 4.

Ziman, J., 2002. *Real science: what it is and what it means*. Cambridge University Press, Cambridge.