

research" in the first bill as a permissible reason to possess anthrax. "The bill ended up being as good as we could expect given the current climate," she says.

The ASM has not established how the proposed second law would affect research on anthrax or other agents in the United States, but it should know soon as it is currently notifying its members of the law's provisions. However, Shoemaker says that "the language in the bill is worrisome".

The second bill also requires any laboratory or individual in possession of a select agent to register with the government within 30 days. The ASM estimates that more than 250 labs in the United States possess such microbes or toxins, but Shoemaker claims that many would have difficulty in compiling a comprehensive list in such a short time. "Some labs might not even know what agents they have in their inventory," she says. The ASM plans to push for more time to comply with the new laws at these Senate hearings.

Elizabeth Marincola, executive director of the American Society for Cell Biology, says that her society is still studying the legislation, but agrees that broad restrictions could be harmful. "These things have to be done surgically, not clumsily," she says.

None of the legislation applies to biological specimens that are not listed as select agents, but because the bills refer frequently to "biological agents", the ASM is concerned that their passage may lead to confusion among researchers about what is actually prohibited.

Despite the recent anthrax attacks, routine shipments of biological specimens and reagents have so far been virtually unhindered in the United States. Norman Schwartz, vice-president of the life-science group at Bio-Rad, a California-based manufacturer of materials for biological research, says that his company's orders are going out as usual.

Efforts to manage the transport of dangerous biological agents are even more fraught with difficulty outside the United States. Around the world, germ banks that house agents such as anthrax are already under pressure to increase security, according to bioweapons experts.

But despite tighter security and restrictions on transport, terrorists bent on obtaining anthrax can still turn to the natural world. Anthrax spores survive in soil for decades, and anyone with moderate training in microbiology can isolate them, Collier points out. "You are never going to be able to eradicate them from nature," he says. ■

Legal provision for electronic eavesdropping ignites debate

David Adam, London

Essential surveillance or intrusive snooping? As governments around the world react to the attacks of 11 September and their aftermath with new anti-terrorism legislation, opinion is divided over whether they are striking the right balance between individual privacy and national security.

The United States, Britain, France and Canada have each prepared such laws, claiming they are needed to track down people who have already committed terrorist acts and to tighten up security. But privacy and other advocacy groups complain that the laws give police and intelligence agencies excessive power to monitor communications, such as use of the Internet, by the population at large.

The USA-PATRIOT Act, signed into law by President Bush on 26 October, for example, does not widen the range of techniques that intelligence agencies can use to intercept and monitor electronic communications — but it makes it easier for the agencies to get legal permission to use the existing techniques.

Under the act, agencies such as the Federal Bureau of Investigation need only show that reading e-mail or sifting through records of electronic traffic held by Internet service providers is "relevant to an ongoing criminal investigation" to obtain this permission from a judge. Previously, they had to convince the judge that the communication to be tapped was linked to actual criminal activity.

In a statement on 11 October, after an initial version of the bill had been passed, Bush said that the new law "respects our constitution" while giving law-enforcement agencies "essential additional tools to combat terrorism and safeguard America against future terrorist attacks".

But some argue that the act lowers the legal barrier to electronic surveillance too far. "There is an obvious risk to privacy every time the standards for government access to personal data are weakened, and in this legislation standards are being substantially weakened, particularly in intelligence investigation," says Jim Dempsey, deputy director of the Center for Democracy and Technology, a Washington-based group that advocates privacy on the Internet.

On 15 October, British home secretary David Blunkett outlined a series of anti-terrorism measures which the government intends to make law by the end of the year. They also include rules to allow easier access to records of electronic communication.

Blunkett's proposals would enable Internet service providers to keep extensive



Listening in: these 'golf balls' in Yorkshire are thought to gather data for British intelligence.

logs of e-mail traffic and Internet use, as they often do in the United States; this is currently prohibited by European data-protection laws. British police already have powers to access such records where they exist.

Similar laws just passed in France mean that records from Internet service providers will be made available to police. And the German Bundestag will debate new security legislation on 7 November, although it is not clear whether it will change the rules safeguarding Internet privacy.

A spokesperson for the British Home Office says that some concerns over the proposed powers are misplaced. "This does not mean that we are going to, or indeed want to, look at people's e-mails," he says. "We're not talking about the content, we're talking about the actual dialogue itself, the record of who communicated with whom."

Internet service providers also hold lists of the web pages (URLs) visited by individuals. Such data will now be more readily available to US and British law-enforcement agencies. British security agencies will only be allowed access to the 'stem' of the URL (such as www.nature.com), but US law enforcers will be able to identify the specific page.

Privacy advocates claim that the changes are equivalent to monitoring which library books someone borrows, and constitute an infringement of civil liberties. But others point out that this type of record can already be sold to commercial organizations to help them target their marketing.

"If companies are storing some of this data anyway for commercial use, then to argue that it's an imposition to provide it under proper authority to law-enforcement agencies strikes me as specious," says James Lewis, director of technology policy at the Center for Strategic and International Studies, a Washington-based foreign-affairs think-tank. ■