Public Interest Law Reporter

Volume 11
Issue 1 *Spring 2006*

Article 11

2006

Can Your Privacy Be Protected in an Internet Age?

Suzanne Blaz

FEATURES

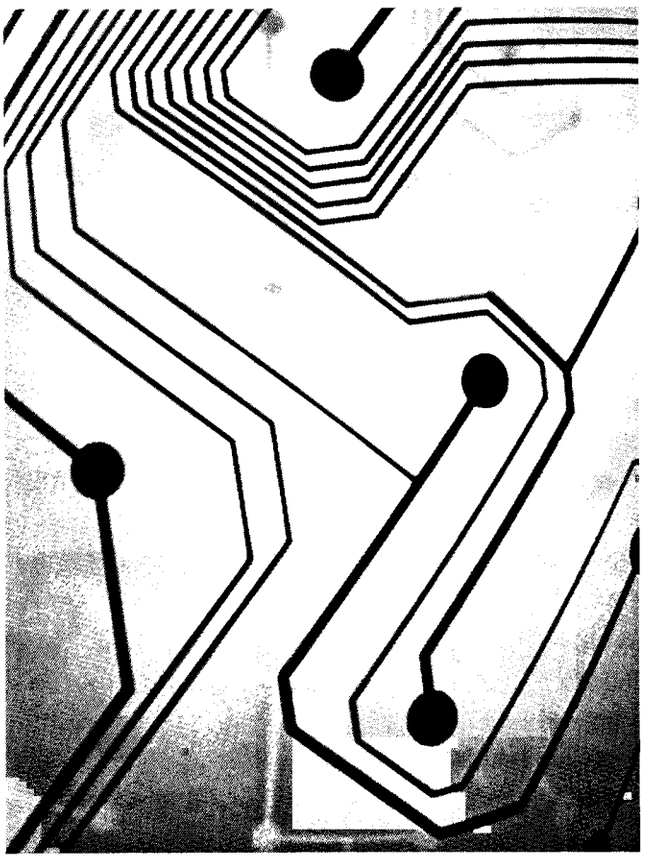
Can Your Privacy be Protected in an Internet Age?

By Suzanne Blaz

In addition to the recently discovered secret wiretapping of American citizens' phones by the U.S. Government,[1] recent advances in Internet and copy protection technology are raising new security and privacy concerns for consumers. Two instances of particular import demonstrate that U.S. Internet and computer privacy may be at risk in the future: Sony BMG Music Entertainment's attempt to protect the copyright of its music by installing a digital-rights-management program onto compact discs, which automatically install onto personal computers without the owner's knowledge;[2] and Google's new desktop software that is designed to help users move and search their computer files, but allows access to this information by Google[3] and perhaps the U.S. government, although the government's recent subpoena for Google's Internet searches was denied.[4]

In the area of cyberlaw, privacy and copyright issues are always of concern;[5] however, the law is not always able to keep up with the technology and can lead to Americans' private information and computers being accessed by others without any recourse.[6] Indeed, as Michael Hiltzik of the *L.A. Times* noted regarding the government's wiretapping, "[i]t's plain that the necessary ingredients for a surveillance program on such a scale are the will and the technology. The law no longer matters, because technology has left it in the dust."[7]

Indeed, many users did not and still do not know that Sony BMG was routinely installing a hidden software program, known as the Extended Copy Protection ("XCP"), on their CDs.[8] This software is essentially a rootkit,[9] a relatively new term that describes a file or folder that is invisible to the user, is hidden from spy-ware or virus searches, degrades the computer's performance and can control critical computer functions, allowing others access to a person's computer. Moreover, it has been deemed "spyware" by Microsoft.[10] This software was exposed when Sony BMG released a utility program to help users remove the rootkit component of the XCP from their computers;[11] however, this program did not effectively remove the rootkit software, but only unmasked the hidden files created by the XCP, and effectively disabled the consumers' computer CD player from being able to play all CDs.[12]



Recent threats to privacy have come from anti-piracy software, internet search engines, and file transfer applications.

Furthermore, the XCP anti-piracy software not only masked its presence, but also introduced a vulnerability that hackers and virus writers began to target, which forced Sony to recall millions of its CDs.[13] The XCP software gave not only Sony BMG, but also hackers, a "back door" to access a user's computer, because the rootkit that it installs, a security tool that can capture computer passwords so that one can access your computer remotely, collects information from a user's personal computer and allows others access to it without the user ever being aware of this access.[14]

Sony BMG issued two public apologies and recalled the CDs, stating, "[w]e deeply regret any

(**Tech Privacy**, *continued on page 18*)

(**Tech Privacy**, *continued from page 17*)

inconvenience this may cause our customers."[15] Steps that Sony has taken to make reparations include a proposed settlement that will pay consumers $7.50 per CD that had the XCP software or allow them three free downloads of whole albums online.[16] Additionally, Sony has stated that it is committed to providing software to help remove the rootkit;[17] however, the program available on its web site to remove the software is not entirely effective.[18]

This incident has not only tarnished Sony's image, but also brought government attention. On February 16, 2006, after speaking with BMG executives, the director of law enforcement at the Department of Homeland Security ("DHS"), Jonathan Frenkel, issued a statement that the DHS may consider outlawing rootkits, stating that, "[the government] need[s] to be thinking about how we ensure that consumers are not surprised by what their software programs do."[19]

In addition to threats from the DHS, Sony BMG faces several lawsuits[20] as a result of the XCP software, one of which was brought by the Electronic Frontier Foundation ("EFF"), a non-profit group that pledges to protect consumers' digital rights.[21] These lawsuits allege, among other things, that Sony BMG violated the federal Computer Fraud and Abuse Act[22] and the federal Electronic Communications Privacy Act[23] in addition to common law invasion of property, trespass to chattels and violation of State fraud acts.[24]

Despite the adverse publicity from the Sony BMG incident, the entertainment industry continues to experiment with rootkits and other programs to try and protect their copyright. For instance, some copies of the movie *Mr. & Mrs. Smith* were released with rootkit programs,[25] and Symantec also developed rootkits to protect its copyright on the Norton Antivirus program it owns.[26]

There are laws that help companies who wish to the protect their copyrighted material from being dispersed to the masses over the internet, such as the Digital Millennium Copyright Act ("DMCA")[27] passed in 1998; however, this law is becoming more controversial and may come under attack in situations where the consumer is harmed. For instance, while the DMCA makes it illegal for users to circumvent digital protection software, it does not address situations where it may be necessary for someone to bypass harmful software, such as the rootkits on the Sony CDS, or in order for consumers to make fair use of the material they bought on different media that they own.[28]

Another security threat that looms over Americans is Google's new desktop program, which lets users automatically transfer information from one personal computer to another and allow them to search their desktop files; however, the user must allow Google to store the material for up to 30 days.[29] This service is available for free, but worries over this service have arisen because of the U.S. government's recent demands for searches made by users of Google's search engine and other information.[30]

Google recently fought the U.S. Justice Department over its subpoena for internet searches, which the government wanted in order to compile data in response to a Supreme Court case[31] that cast doubt on the constitutionality and effectiveness of the Child Online Protection Act ("COPA").[32] The Supreme Court case is currently blocking COPA's usage in order to protect free speech rights.[33] The Justice Department also asked for a random sample of one million Web pages that can be searched through Google's site.[34]

Google argued that it would not comply with the request because it gave the government unbridle access to information about their users violating their privacy, and also because compliance with the subpoena would expose Google's trade secrets.[35] Additionally, Google argued that the government failed to demonstrate that the information would even be admissible evidence in court.[36] Other companies, such as AOL and Yahoo, chose not to fight the government and complied with the request for their Web pages and user's search information already.[37]

On March 17, 2006, U.S. District Court Judge James Ware ruled that Google was not required to provide the internet searches, but was required to work with the government to construct a way to randomly obtain 50,000 Web Pages that could be handed over.[38] The Court ultimately granted part of the Justice Department's request because it was narrowly tailored, but gave Google time to file objections to this order if

(**Tech Privacy**, *continued on page 28*)

FEATURES

Bioshield 2: A Shot in the Right Direction?

By Lindsay Frank

Despite the introduction of the Biodefense and Pandemic Vaccine & Drug Development Act of 2005 ("Bioshield 2"),[1] pharmaceutical companies are still reluctant to enter into the business of mass-producing vaccines,[2] and critics of the bill condemn the blanket liability protections it provides to these companies.[3]

Introduced by Sen. Richard Burr (R-N.C.) on October 17, 2005, Bioshield 2 was approved by a voice-vote the next day by the Senate Health, Education, Labor and Pensions Committee.[4] Bioshield 2 will allow drug companies to bypass typical testing procedures for new vaccines and drugs in case of an avian pandemic flu outbreak or bioterrorist attack.[5] Moreover, Bioshield 2 aims to shield the pharmaceutical companies who develop the vaccines against personal injury lawsuits brought by individuals suffering from adverse reactions or side effects caused by the vaccine.[6] The bill would offer 10-year market exclusivity to drug companies, which would prevent competitors from developing more affordable generic alternatives.[7]

This bill replaces the original Bioshield II legislation that was designed by Sens. Joseph Lieberman (D-Conn.) and Orrin Hatch (R-Utah).[8] Bioshield II died because its "wild card" patent provision would have allowed pharmaceutical companies developing bioterrorist countermeasures to extend patents on their popular and exceedingly more profitable drugs, even if those drugs were unrelated to the production of countermeasures.[9]

Planning a national defense against bioterrorism and pandemic disease has proved contentious among politicians, pharmeceutical corporations, and public interest groups.

For several years, the Bush Administration has desired that pharmaceutical companies increase their production of biodefense countermeasures with little or no incentives.[10] In fact, shortly after the anthrax attacks in 2001, the Center for Disease Control ("CDC") asked Bayer Pharmaceutical, the makers of Cipro, to get the FDA to approve the drug as a treatment for anthrax.[11] Bayer acted in accordance with this request at their expense and further donated four million doses of Cipro to the government.[12] However, Bayer refused to comply with the government's subsequent demand of an additional one million doses at a discounted price, despite threats to suspend their patent on Cipro.[13] Recognizing the need to provide pharmaceutical companies with greater incentives, Project Bioshield was signed into law in 2004.[14] The law provided the government with $5.6 billion over the next 10 years for the purchase of vaccines and countermeasures designed to protect Americans against anthrax, small pox and a chemical, biological, radiological or nuclear ("CBRN") attack.[15]

Despite the incentives to lure certain drug makers into the biodefense and pandemic flu market, very few of the large pharmaceutical companies jumped at the opportunity to accept the grants offered by the government.[16] One reason for their skepticism was the probable cost of approximately $800 million to $1 billion to develop a new drug without a guaranteed market for it.[17] Additionally, the large pharmaceutical companies did not avail themselves of the grant because they were reluctant to divert research from their popular and highly lucrative drugs to those that are stockpiled and used in the event of an unlikely emergency.[18] The pharmaceutical industry was also concerned with potential liability for administering bioterror drugs that cannot first be tested on humans.[19]

(**Bioshield 2**, *continued on page 20*)

(**Bioshield 2**, *continued from page 19*)

In response to the lack of eagerness from larger pharmaceutical companies, some of the smaller pharmaceuticals companies have stepped up to the challenge in order to obtain a government contract.[20] Yet, in some instances, their tremendous efforts and equally high expectations have been met with disappointing results.[21] For instance, Hollis-Eden Pharmaceuticals, a small company located in San Diego, experienced first hand what many other companies had feared most.[22] The company eagerly pursued what would be its first government contract and spent more than $100 million to develop Neumune, a medicine designed to combat acute-radiation sickness.[23] Yet after the Department of Health and Human Service's ("DHHS") initial request for bids, Hollis-Eden learned that the government only planned to buy 20,000 to 200,000 doses of their drug.[24] This number severely conflicted with what many industry watchers believed would be a proposal for doses numbering in the millions.[25] While the DHHS eventually stated that this was only a preliminary number,[26] it is not surprising that many companies have shied away from the potentially devastating risks in order to set their sights on more predictable and profitable endeavors.[27]

Yet after increased fears of another biological threat, avian flu, began to surface, the Bush Administration pushed for measures to fix some of Project Bioshield's highly criticized provisions.[28] Due to exceedingly high expenses and potential liability, the major pharmaceutical players pressed the legislature for more incentives to encourage entry into the speculative market of bioterrorist and pandemic flu countermeasures.[29]

Accordingly, Bioshield 2 was developed and proposes to create a new federal agency called the Biomedical Advanced Research and Development Agency ("BARDA") that would promote and coordinate "advanced research and development of drugs and vaccines in response to bioterrorism and natural disease outbreaks."[30] Moreover, BARDA would further streamline the approval process for biodefense products and assist companies from the early stages of product development until they are ready to bid on a government contract.[31] Currently, the Department of Homeland Security is responsible for developing bioterrorism countermeasures.[32] Under Bioshield 2, BARDA would be protected from the Federal Advisory Committee Act and the Freedom of Information Act, which has sparked much controversy over the bill.[33] The Federal Advisory Committee Act ensures that advice given to the executive branch[34] is also given to the public, while the Freedom of Information Act requires federal agencies to make their records available to the public to the extent that they are available.[35] Instead, BARDA would be supervised by a political appointee and proposes to allow the research and development behind vaccines to be kept secret from the public.[36] Additionally, evidence of deaths and injuries occurring from drugs and vaccines labeled as "countermeasures" would also be kept under wraps.[37]

"It's appalling that in the guise of a health-related bill, the government is giving the vaccine industry unprecedented immunity for the harm that their product can cause."
-Amber Hard, staff director for the Center for Justice and Democracy

Bioshield 2 comes in wake of a $7.1 billion strategy outlined in November 2005 by the Bush Administration to expand and accelerate pharmaceutical companies' capacity to produce vaccines within the United States, stockpile treatments against the H5N1 avian influenza A virus, and detect and respond to a pandemic flu outbreak.[38] In addition, Congress passed a defense bill last December that included $3.8 billion, "mainly for flu vaccines and medicines."[39] The Bush Administration is hopeful that the new legislation will appease the pharmaceutical industry and enable companies to produce enough vaccines for every American within six months of the start of a pandemic outbreak.[40]

Proponents of the bill argue that a liability waiver is essential to avoid frivolous lawsuits, which they attribute to hindering the progress of vaccine

(**Bioshield 2**, *continued on page 21*)

FEATURES

(**Bioshield 2**, *continued from page 20*)

developments in recent decades.[41] They also assert that a victim suffering from harmful side effects stemming from a pandemic vaccine will not be left without a viable remedy as the legislation plans to provide for a compensation fund modeled after the Smallpox Compensation Fund.[42] The fund would allow injured victims and their families to apply for death benefits, lost income and medical expenses.[43] In addition, the DHHS has the right to waive the liability shield if a pharmaceutical company is found to have willfully neglected the risks associated with their product.[44] Critics of the legislation, including health, consumer and union groups,[45] believe that pharmaceutical companies' expressed fear of lawsuits is misplaced and merely a way to avoid compensating injured victims.[46] In fact, only 10 lawsuits have been filed against makers of influenza vaccines in the past 20 years.[47] Additionally, despite the seeming lack of enthusiasm from many pharmaceutical companies towards Bioshield,[48] the threat of lawsuits has not inhibited some major manufactures of vaccines against influenza such as Merck, Roche, Wyeth, Novartis and GlaxoSmithKline from investing millions to increase their stockpile.[49] In particular, vaccine manufacturer Santa Fe Pasteur has spent $150 million to double its production capacity.[50]

Many Democrats opposed to the legislation argue that Bioshield 2's liability protections are detrimental to the public's best interest without a sufficient compensation fund for those injured by the vaccine.[51] Although Republicans believe that a compensation plan should be set up for "first responders," many assert that it is nearly impossible to set up a fund for those who take the drugs after a bioterrorist attack, as compensation needs would be contingent on the circumstances of each situation.[52] This rather laissez faire approach to a compensation policy is what worries critics who have compared the lack of a tangible fund to the ultimate failure of the Smallpox Vaccine and Compensation Act of 2003.[53] The Act was designed to pursue the ultimate goal of vaccinating approximately 500,000 public healthcare workers against smallpox, but was unsuccessful largely because of the government's failure to execute a legitimate compensation plan.[54] As a result, only 40,000 healthcare workers actually took part in the vaccination program.[55] Similarly, without a legitimate compensation fund, critics of Bioshield 2 assert that Americans will be largely hesitant to take these drugs in the event of a biological attack or pandemic outbreak.[56]

According to Amber Hard, staff director for the Center for Justice and Democracy in Illinois, "[i]t's appalling that in the guise of a health-related bill, the government is giving the vaccine industry unprecedented immunity for the harm that their product can cause." [57] Hard went on to say that Bioshield 2 "makes all of us living guinea pigs and gives pharmaceutical companies carte blanche to develop drugs [that may not be safe for the general public]."[58]

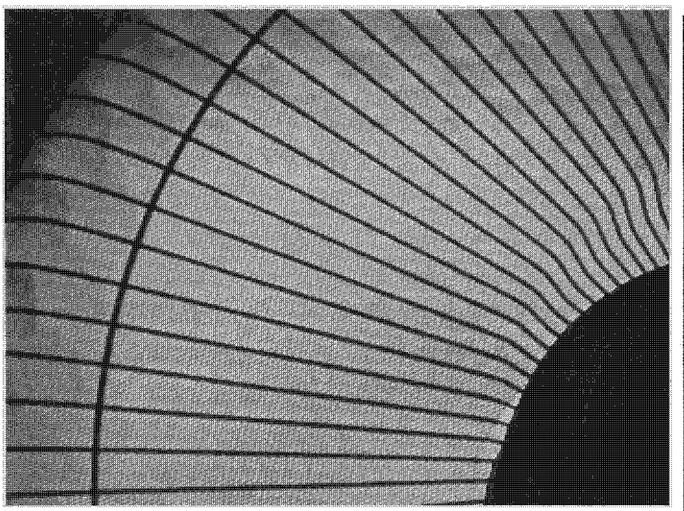
This is not the first time the government has shielded pharmaceutical companies from liability against lawsuits. Over the past 30 years, the government has issued major liability protection and compensation programs such as the National Swine Flu Immunization Program of 1976,[59] the National Childhood Vaccine Injury Compensation Act of 1986[60] and the Phase I Smallpox Vaccination Program that was launched in 2003.[61] Yet the National Swine Flu Immunization Program of 1976 did not limit the amount of compensation recoverable by victims.[62] Rather, this Act required injured victims to file their claims against the government after filing an administrative claim.[63] The government was then able to "seek indemnification from negligent parties covered by the liability protections."[64] The National Childhood Vaccine Injury Compensation Act of 1986 allowed injured plaintiffs to go to court if they were not satisfied with the administrative result and merely disallowed punitive damages so long as the company had complied with the Federal, Food, Drug and Cosmetic Act and the Public Health Service Act.[65] Finally, the more stringent restrictions imposed by the smallpox vaccination program proved catastrophic to the legislation as people refused to subject themselves to the vaccine without the possibility of adequate compensation.[66]

Similar to those opposed to the Smallpox Vaccination Program, critics of Bioshield 2 argue that the bill places too much emphasis on protecting

(**Bioshield 2**, *continued on page 30*)

Sharp Increase in Heating Prices and Limited Government Assistance Spark Concerns about Potential Home Heating Crisis

By Claire Mariano



While volatile energy prices have prompted the federal government to increase its funding of the Low-Income Home Energy Assistance Program, spending is still $2 billion below the program's dicretionary limit and does not serve over 25 million poor households.

High energy prices and continued debate over funding for the Low-Income Home Energy Assistance Program ("LIHEAP")[1] has led to an outcry from advocacy organizations, some elected officials and others concerned with affordability of winter heating bills for low-income families. The U.S. Department of Energy's Energy Information Administration ("EIA") estimates that households heating with natural gas will spend, on average, $257 more in fuel costs this winter, about a 35 percent increase from last winter.[2] For households using heating oil, the EIA estimates that these households will average about $275, or 23 percent, more in heating costs when compared to last winter.[3]

Behind these market shifts, the EIA cites weak natural gas production, decreased natural gas imports, high natural gas demand and high oil prices.[4] In addition, Aviva Aron-Dine, representative of the Center for Budget and Policy Priorities, noted that "heating costs have increased for a variety of reasons this year, but the disruptions caused by Hurricanes Katrina and Rita certainly have played a significant role."[5]

An Increased Energy Burden on Low-Income Households

Advocates for low-income families and public policy organizations argue for greater LIHEAP funding by analyzing the heavy energy burden on low-income households.[6] LIHEAP provides basic bill payment assistance for heating and cooling costs, as well as some funding for weatherization programs.[7] Despite the dramatically increased energy costs, LIHEAP funding is appropriated at essentially the same level this year, and current projections mean that the low-income households will likely pay the difference.[8]

According to Economic Opportunity Studies, families in poverty will spend about 25 percent of their Fiscal Year 2006 income on energy bills.[9] There are about 13 million such households in poverty, and there are about 33 million people considered LIHEAP-eligible.[10] For the LIHEAP eligible population, energy bills will consume about 16 percent of their annual income.[11] The burden on low-income households can be contrasted with median-income households, whose average income was just over $47,000 in 2005.[12] Median-income households will need to spend more than 5 percent of their annual income, after adjusting income for inflation.[13]

"Instability with the cost of energy (especially natural gas) is most worrisome for low-income families, whose tight budgets allow little flexibility in spending," said John Colgan, Director of Public Policy for the Illinois Community Action Association. "Winter heating costs can easily push low-income households into a cycle of increasing debt and/or service disconnections."[14]

(**Energy Assistance**, *continued on page 23*)