Testimony of

Edward Black

October 31, 2007

Hearing of the
United States Senate
Committee on the Judiciary
"FISA Amendments: How to Protect Americans' Security and Privacy and
Preserve the Rule of Law and Government Accountability"
Wednesday, October 31, 2007
Testimony of Edward J. Black
President and CEO
Computer & Communications Industry Association

Good morning, Mr. Chairman and Members of the Committee. My name is Ed Black. I have served as President and CEO of the Computer and Communications Industry Association for the past 12 years. CCIA is a nonprofit membership organization for a wide range of companies in the computer, Internet, information technology, and telecommunications industries. Since its founding in 1972, CCIA has consistently promoted innovation and competition through open markets, open systems, open networks. We appreciate this opportunity to help find the best balance of national security law and privacy rights.

The Internet is an unprecedented and unique force for democratic change and socioeconomic progress. Increasingly, our nation's digital economy depends on the dynamism and openness of the Internet. That functionality is jeopardized if surveillance activities result in the chilling of free speech. In our society, all information services companies play a custodial role in promoting First Amendment rights. Internet functionality is further jeopardized if end users lose confidence in the security of their business and personal transactions online. The Fourth Amendment is key to preserving that privacy and network security. While constitutional considerations should be paramount, I will also emphasize some very practical business aspects of this debate over amendments to FISA.

We understand our industry's technology and the many wonderful ways in which can be used... and ways it can be misused. In addition to the most obvious domestic benefits, it can be a tool for spreading freedom and democracy around the world, and from a foreign relations standpoint, the U.S. government needs to lead by example in promoting the freedom of ideas and communications that the Internet makes possible. However, that leadership will fall flat if we easily excuse unlawful surveillance in our own country. We urge you to consider that this legislation could weaken the hand of American companies that must contend with escalating demands for censorship and surveillance by foreign secret police.

CCIA supports current legislative efforts to amend FISA to achieve a sound balance between effective terrorist surveillance for our national security and Fourth Amendment privacy rights of Americans, while enhancing opportunities for the exercise of First Amendment freedoms. We should all want protection both from terrorists and from illegal spying, search and seizure by our own government. In crafting our efforts to combat terrorism, we should not forfeit our privacy or weaken our First or Fourth Amendment rights. As a nation, we should not countenance the sort of autocratic surveillance of ordinary citizens which we find so abhorrent in repressive foreign regimes. American electronic communications and information services companies understandably want protection from overreaching government demands to participate in illegal wiretapping or data mining. We want to be good citizens, but not police agents. But we need protection not just from third party liability for acquiescing to proper demands, but protection from improper government pressure or inducement as well. Industry needs clear constitutional ground rules that are subject to waiver only through transparent procedures and process.

It might be useful to examine and compare how government agencies and the private sector deal with user/customer communications data and content. Of necessity for the provision of public services, government collects certain basic information on taxpayers, citizens, and businesses and other organizations that cannot be legally withheld by the individual or organization. Government agencies, recognizing the importance of privacy, observe many security procedures to protect personal privacy, but too often we have seen serious breaches in this security. Indeed, data mining, hacking, and inadvertent dissemination of information on U.S. citizens creates increasing security challenges for government at all levels. For the government, use of the information, not its confidentiality is paramount.

Internet commerce and the digital economy, on the other hand, fundamentally depend on maintaining the privacy and security of customers' personal information and business data. Private sector companies have information on customers that those customers expect will be kept private, unless they give consent, or a court order of some kind compels release of that personal information to law enforcement. Citizens seem willing to provide vast amounts of data to private institutions believing that these institutions act as a buffer between them and the government. Customers must be free to conduct their personal lives and business transactions without fear of illegal or widespread surveillance and spying. The high-tech industry wants to help our government protect Americans from terrorists. However, companies cannot provide such assistance if network security is compromised because the rules for wiretapping and surveillance are expendable at the discretion of the President, or subject to ongoing controversy and flux. In a sense, the economic and social consequences of a reduction in network security would be a partial victory for the very terrorists we are seeking to defeat.

To be sure, the Director of National Intelligence (DNI) requires the assistance of private communications companies. But those companies must be free to insist on constitutionally solid procedures that are clear and transparent, so they are not reduced to guesswork about the applicability of immunity under the FISA statute. Clear lines of separation and differentiation between public sector and private sector roles in surveillance activities are therefore essential to a robust Internet and a free society.

Private companies, be they in health care, financial services, hard goods retailing, or information services should not become arms of the federal government, regularly turning over customer information, or "sitting on" phone lines. The many companies which are part of our Internet and communications systems must be trusted carriers and repositories of Americans' free speech. Commercial telecommunications and Internet services are not fair territory for direct involvement by the federal government. Put another way, outsourcing to private companies the collection of Americans' call records and communications messages for government use is both unconstitutional and destructive to valuable, and indeed essential, network security.

The role of private sector institutions as a vigilant buffer between excessive government demands and the rights of our customers is a role to be protected, not undermined.

In the interest of national security there is broad agreement on our government's
right to conduct surveillance of foreign targets, especially terrorists, and to collect and share such information even when obtained without court approval. FISA was created for the express purpose of limiting executive privilege regarding surveillance of U.S. citizens. The FISA Court and the Attorney General provide checks and balances in this separation of powers. Since 9/11 2001, the Bush Administration has had many years to work with Congress on important revisions to the FISA law. That opportunity was squandered, however, in favor of a unilateral secret National Security Administration (NSA) spying program. When high-level internal debate ensued over the legality of that program, it was covered up. Even the private sector companies who were being asked to assist may not have been aware of the controversy.

CCIA believes that HR 3773, the RESTORE Act of 2007, which is now under consideration in the House of Representatives, offers careful and enlightened updating of FISA. The Senate Intelligence Committee legislation, S. 2248, while providing some important improvements over the hastily passed Protect America Act (PAA) of last August, allows surveillance based on executive certification, without a court order. And, disturbingly, the bill provides retroactive immunity from civil liability for those who may have participated in an illegal program, without identifying what conduct is being immunized.

The Executive Branch has the primary burden to establish that requests for data are on strong legal footing, under the Fourth Amendment and FISA, and do not amount to illegal search and seizure of U.S. citizens private information. But the Bush Administration apparently did not present independent judicial legal authorization to some of the companies involved. The Administration simply "certified" the program was legal. And some very large companies with legions of their own lawyers either did not double check, or, well, we just don't know what transpired. Apparently Qwest did run a legal reality check, and concluded some of the executive requests were out of line. Whatever letters were used to request assistance have not been shared with the House Judiciary Committee or any Member of the House of Representatives to date. Senate Intelligence Committee members only merited a limited look at these documents immediately prior to their vote on S. 2248. We understand that the leadership of the Senate Judiciary Committee, after a year of ignored or rejected formal requests, finally was offered a look at some of the relevant documents late last week. But none of us know about what type of debates, if any, took place between the government and the companies involved, or within the companies.

We think there are important lessons that can be learned from what has transpired over the last several years. Learning these lessons will help us draw the lines of proper conduct for the future. Alternatively, if we make up the rules as we go along, ANY violation of the constitution performed to serve a compelling national security or law enforcement purpose can be rationalized and covered up by retroactive immunity. Under this scenario, private industry effectively becomes the judge, weighing whether particular purposes are sufficiently compelling to risk unconstitutional searches. The government doesn't want that; neither do we.

Retroactive immunity for participation in the recent secret government surveillance program is premature at best, since this Congress has yet to become well-informed enough to determine whether in fact the NSA surveillance program exceeded legal boundaries established under FISA. If immunity for past activities is granted prior to full disclosure and accountability from the Executive Branch, Congress and the public may never understand the nature of the NSA warrantless wiretapping program. We also believe broad retroactive immunity would be ill advised in any event because it would perpetuate uncertainty, confusion and second-guessing in the future. Commercial enterprises and individual employees have the right to insist on clear judicial authorization before complying with requests for information or communications otherwise protected by customer privacy guarantees. And companies would know that in getting judicial authorization, they will avoid having to petition for additional extrastatutory immunity later. But if retroactive immunity is granted in this case, future extralegal emergency requests will beaccompanied by a wink and a promise of similar immunity after things settle down.

Understandably, some companies want this immunity badly. Their motives may have been as honorable as their legal analysis was lax, but we don't know enough at this point to make a judgment. We do know, however, that some of the companies involved, when they want something from the government, be it immunity from liability or further deregulation, tend to threaten a parade of horribles that will arise if they are not granted the desired relief. When the prize is sweeping deregulation, we hear that without it, they will have no more incentive to invest in broadband network infrastructure. When the goal is immunity from participation in the NSA program, they threaten that without it, they will be reluctant to co-operate in the future. But as long as electronic communications companies are presented with clear legal authorization in the future, they should have every reason to provide the network assistance that is so important to our national security. Hence, Congress must establish bright, constitutional lines identifying industry's responsibility.

With regard to claims of possible bankruptcy, it makes sense for Congress to at least consider a statutory cap on damages that might be awarded to plaintiffs for information wrongly provided in a past NSA program, especially following a finding of good faith by a federal judge. In any future consideration of immunity from liability for participation in government surveillance, small businesses and individuals should have a lighter burden of establishing they acted in good faith in a response to a high-level government request.

The civil litigation should be allowed to proceed. Even if major portions of the proceedings need to be held in camera and the scope of discovery narrowed, judges - and to the extent compatible with serious national security concerns, the public - should learn what really happened in these cases.

Conclusion

Millions of workers in our industry believe that we are an industry that can be strong positive force for our society. The underlying desire to facilitate communications, the transfer of information and knowledge, and the building of bridges

across cultural boundaries: these are core motivations of people in our industry. These motivations are part of why our industry is successful. The economic rewards can be great but they are as much a consequence as they are a motive.

To sustain this positive force, we must work together to establish processes and protections for private personal and business information that is so critical to the open and free use of the Internet. To disclose private information, our industry needs clear and constitutionally proper ground rules that are only deviated from through well-defined transparent processes. These rules must be straightforward enough to be publicized and understood by U.S. citizens and businesspeople who may be called upon to assist their government in these uncertain times.

NOTE: The views expressed herein do not necessarily represent the position of every individual CCIA member company.