

2002

Orwell's Prophecy

David M. White
Western Kentucky University

Follow this and additional works at: http://digitalcommons.wku.edu/stu_hon_theses



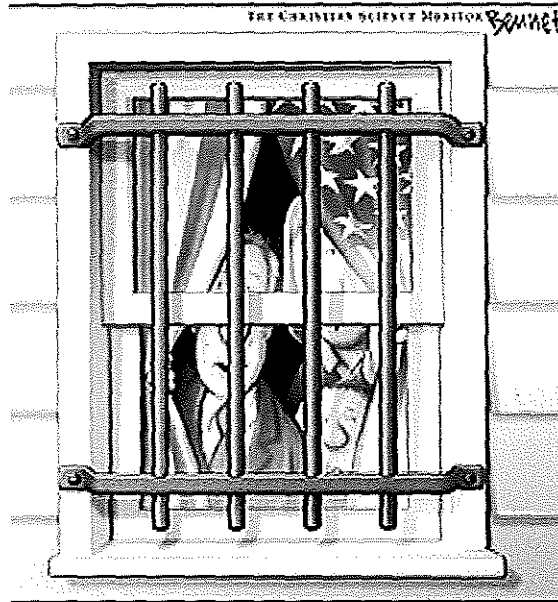
Part of the [Social and Behavioral Sciences Commons](#)

Recommended Citation

White, David M., "Orwell's Prophecy" (2002). *Honors College Capstone Experience/Thesis Projects*. Paper 175.
http://digitalcommons.wku.edu/stu_hon_theses/175

This Thesis is brought to you for free and open access by TopSCHOLAR®. It has been accepted for inclusion in Honors College Capstone Experience/Thesis Projects by an authorized administrator of TopSCHOLAR®. For more information, please contact topscholar@wku.edu.

Orwell's Prophecy



'I guess it was easier than putting the terrorists behind bars.'

Senior Honors Thesis

Presented to the University Honors Program

Western Kentucky University

Bowling Green, KY

April 2002

David M. White

Approved by

Stephen B. Groce

Walter R. ...

Patricia A. ... 5-16-02

Table of Contents

Abstract.....	i
Acknowledgements.....	ii
Introduction.....	iv
Chapter 1: Language.....	1
Chapter 2: Big Brother Is Watching You.....	28
Chapter 3: The Hope for Humanity.....	54
Bibliography.....	59
Appendices.....	63

Abstract

Even though the year 1984 has come and gone without a totalitarian dictatorship having come to power, George Orwell's predictions in *1984* are still hauntingly relevant in today's world, specifically regarding the effects of language on society and the invasion of privacy made possible by advancing technologies. Orwell's frightening dystopian society of Oceania bears a striking resemblance to present-day America. The United States has been set on a course towards Oceania for some time now. It is becoming alarmingly apparent that the tragic events of September 11th may well prove to be the final catalyst needed to turn America into Oceania. By heeding Orwell's warnings, Americans can perhaps avoid the impending dystopia that he prophesied or, at the very least, not be caught looking the wrong way when it finally does arrive.

Acknowledgements

The following Senior Honors Thesis would not have been possible had it not been for the contributions of so many people throughout my five years here at Western Kentucky University. I would like to express my gratitude to the following people and groups of people:

- God for having blessed me with so many gifts.
- My parents for all of their emotional and financial support over these past five years, which were probably harder on them than they were on me.
- My eleventh grade AP English teacher, Dr. William McCabe. His class was without a doubt the most influential class I ever took in high school. It made me who I am today. O captain, my captain!
- The WKU Honors Program for the scholarships it has awarded me.
- The Honors Thesis Coordinator, Walker Rutledge. I know I'm not the easiest person to work with, and all of my seemingly redundant revisions must have driven him nuts and at times made him feel unappreciated for all the time he invested in me.
- Dr. Carl Kell of the WKU Communications Department. I could always count on him for warm support and perspective whenever I was lost. Thank you.

- Dr. Edward Bohlander of the WKU sociology department for all of the guidance and support he has given me throughout my years here at Western. I also wish to thank him for simply putting up with me. After all, as he once told me, “Mr. White, you’re the only student I’ve ever had who gives me short-answer responses on multiple-choice tests!”
- My thesis director, Dr. Steve Groce, also in the WKU sociology department, deserves special mention here. Without the academic foundation he provided for me in his sociological theory class, this thesis never would have been possible. For it was in that class that I finally began to see the world through the eyes of a sociologist. He constantly challenged me to think in new ways.

Introduction

Some say George Orwell can be ignored now that the year 1984 as long since passed, without the dystopian society that he envisioned ever having taken full form. On the contrary, Orwell's prophetic vision is timelier than ever before, specifically on the subjects of language and privacy.

Orwell's frightening dystopian society of Oceania bears a striking resemblance to present-day America. The United States has been set on a course towards Oceania for some time now. The events of September 11th may prove to be the final catalyst needed to transform present-day America and, indeed, the rest of the world, into the dystopian society that Orwell feared.

By laying the template of Oceanic society over present-day America, one discovers the insights that have long since been buried and forgotten in the pages of *1984*. By heeding Orwell's warnings, Americans can perhaps avoid the impending dystopia that he prophesied or, at the very least, not be caught looking the wrong way when it finally does arrive.

Language

"Language is the armory of the human mind, and at once contains the trophies of its past and the weapons of its future conquests." - Samuel Taylor Coleridge

Those who master language are confronted with a terrifying freedom. For language has as much ability to enslave as it does to free. It can breathe life into a society, or it can suffocate it, providing only small pockets of oxygen for the fortunate few. George Orwell reveals with often disturbing clarity just how powerful a tool language can be in the wrong hands. His concern is psychological manipulation through the debasement of language. In his own terms found in "Politics and the English Language," Orwell suggests that if "thought corrupts language, language can also corrupt thought."¹ He presents power as a means of controlling language and ultimately human thought.

Essentially, the concept of linguistic relativity is what Orwell explores in *1984*. This concept is academically known as the Sapir-Whorf hypothesis, which suggests that the language people use determines their worldview, that it shapes their reality, often times without their knowledge and consent. Whorf proposed: "We cut nature up, organize it into concepts, and ascribe significances as we do, largely because we are parties to an agreement to organize it in this way- an agreement that holds throughout our speech community and is codified in the patterns of our language." And in the words of Sapir: "Human beings...are very much at the mercy of the particular language which has

become the medium of expression for their society...the fact of the matter is that the 'real world' is to a large extent unconsciously built up on the language habits of the group."²

One parallel between Oceana and America is the concept of free thinking being a disease. In Oceanic terms this is often referred to as "symptoms of unorthodoxy."³ The current commercialization of patriotism in the US is a prime example. In the immediate weeks after September 11th, one could buy American flags, pins, bumper stickers, clothes, etc....Wearing an American Flag lapel pin or displaying the flag on one's car or in one's home was considered the patriotic thing to do. Anyone who refused was considered to be unpatriotic and unsympathetic.



Those in America who do not conform to the cultural trance of pop culture are looked down upon by those who do. Each group considers the other to be the outcast group. Such social structuring often begins in elementary school, with the formation of the infamous social rivalry between the "nerds" and the "cool kids." Often, the cool kids are the ones who have the newest video games and know all the words to the popular

songs. Once these kids hit high school, their new goal is to have sex. Those who do are presumed mature and given immediate social status as being popular, because that's the ideal set forth in popular network TV shows and on MTV especially.

Marshall McLuhan, in his landmark book *Understanding Media: the Extensions of Man*, maintains that TV has become a cultural commodity, one readily accepted as a social bond. As such, when people break this bond, or social norm, it is viewed upon by the larger group, or the group with the most social influence, as a form of social deviance.

It can be argued that American popular culture is the verbal assassin of the English language. It seems that all college students use the same catch phrases and, when they want to be funny, will use a line from a popular teen movie. For example, nowadays, when college students ramble on and on with little stories, the cute way for someone else in the group to let them know that they're being annoying is to say, "And one time, at band camp..." which is a line from the hit teen movie *American Pie*. This is as opposed to simply saying, "We understand." Essentially, students are only using corporate America's prepackaged thoughts when they want to communicate. One might argue that pop music and movies, along with MTV and all of its "unique" and "original" programming, are turning the current generation into an army of mindless, Pavlovian robots, with the same agenda: fame, money, power, and sex. As a result, the slovenliness of our language makes it increasingly easier for us to have foolish thoughts.⁵ People who think foolishly are easily led by an elite few.

The stage is set for imprecise thinking at an early age. The majority of babies born in the US are placed into daycare within one year so that their mothers can return to work. American preschoolers spend a great deal of time watching TV, which results in

children missing both the personal interaction and language content tailored to each child's developmental schedule. Truthfully, we really don't know how many children are being told to "be quiet" by stressed-out caretakers, by parents who are pressed for time, or by baby-sitters who have poor mastery of English and who would rather be watching the soaps.⁶ Thus, it is disturbingly possible that untold numbers of American children may already be in intellectual jeopardy before they even start grade school.

Many teachers blame the problem of fuzzy thinking on children not reading enough. As said by one English teacher at an independent school in Ohio:

My students? Well, they don't read. The culture doesn't read. They don't use language above the colloquial expressions because the mainstream culture is dangerously indifferent to the importance of precise language. I don't have much hope of producing readers in the classroom until we can produce readers in the larger social context. I used to be able to use *Tale of Two Cities* in a good eighth-grade class; now, even with ninth graders I approach it warily. If they read it on their own, they miss the connections and so much of the meaning—particularly the subtle ideas. The syntax is just like a foreign language to them.⁷

According to Jane Healy, author of *Endangered Minds*, SAT verbal scores have been steadily declining since 1964, and at a far greater rate than math scores. Steady increases in TV viewing and less time spent reading are readily accepted as negative influences on verbal scores. Eighty percent of the books in this country are read by about ten percent of the people. In fact, Healey suggests that "the act of reading itself may well be on the way to obsolescence."⁸

In 1984, the "telescreen" is a device used to spread The Party's propaganda to all Oceanic citizens while simultaneously keeping the entire population under twenty-four-hour audio and video surveillance.⁹ The privacy aspects of the telescreen in modern-day society will be addressed in the next chapter. What is of linguistic concern here is the

apparent numbing effect of television on the brain. Evidence suggests that TV has the following effects on learning: (1) some television and videotape programming artificially manipulates the brain into paying attention by violating certain of its natural defenses with frequent visual and auditory changes (known as “saliency”); (2) television induces neural passivity and reduces “stick-to-it-iveness”; (3) television may have a hypnotic, and possibly neurologically addictive, effect on the brain by changing the frequency of its electrical impulses in ways that block active mental processing.¹⁰

People who have undergone deliberate hypnosis can attest to the fact that when they are “under,” their brains can absorb anything. This information can be good or bad. In the case of the mass media, this is bad, because if viewers’ brains are hypnotized while they are watching TV advertisements, for example, then they are more suggestible, and that much more likely to go out and buy whatever product they see. Politicians benefit from this effect because viewers are more vulnerable to them. Many people complain that politicians are too boring. This may, in fact, be a deliberate move on their part, because if they “put us to sleep” with their boring, repetitive rhetoric, then even though we’re consciously tuned out to what they’re saying, our brains are nevertheless still more relaxed and can absorb information more easily. Consequently, we’re subconsciously more accepting of their messages, for better or for worse. The Party knows this in Oceania. It’s also quite possible that the power elite in the US know it as well, and probably have for quite some time.

A. Jane Hamilton, a middle-school teacher from Hillsboro, NH, provides further evidence of this trend when she describes her class:

Sitting facing the television, muttering half thoughts or reactions into black space—this is the primary linguistic training ground for most

of my students. There is no meaningful interaction. I have before me a generation of youngsters whose world encourages linguistic passivity.¹¹

“Our society is becoming increasingly *aliterate*,” warns Dr. Bernice Cullinan of New York University. “Most aliterates watch television for their news, but the entire transcript of television newscast would fill only two columns of the *New York Times*. Aliterates get only the surface level of the news.”¹²

Wonders Healey, “Is it possible that reading is becoming an unnecessary relic of a passing culture? Could new habits possibly be more adaptive for today’s kids or for society? Do we really want policymakers who are untroubled by the weighty realities of history because they have never read—or reflected—about them? Or voters who have never peeked around the corner of their own thinking?”¹³ Indeed, this is exactly what The Party wanted in 1984. It can also be argued that this is also consistent with what the power elite in the US want—an unquestioning and malleable public consciousness, or unconsciousness.

Todd Gitlin, in his book *Media Unlimited*, further examines the dumbing down of the English language in the mass media. One logical explanation is that American life is increasingly moving at an exponential pace. Americans have less and less time to devote to old-fashioned reading, while multimedia presents itself as an increasingly viable alternative to satisfying all the informational needs a person could ever have. Authors realize this, and more importantly, so do their publishers, who cut their paychecks. As vocabulary range is reduced as a result of people no longer needing to know a lot of words in order to obtain timely information, sentences are now simpler and far less challenging to mentally digest. This simplification makes modern novels more accessible

to the average reader, and thus a more plausible purchasing option. Not surprisingly, it appears that this effect is compounded over generations.

Another possibility offered by Gitlin is that more and more authors are trying to get their novels turned into movies. As a result, writers are tailoring their novels to fit the screenplay format and the general linguistic trends in the movie business. They are cashing in on the cultural capital of the English language. It's no accident that Tom Clancy holds the sentence brevity record for *Executive Orders* (1996), with a total of 23 words spread out over four sentences. Gitlin explains why:

Accomplished language is an impediment. The less distracting the language, the more exportable the product. Non-English-speaking audiences, now expected to deliver a large chunk of box office revenues, will not be troubled by clichés or grunts- or so it is believed. Given the high offshore returns even from action movies like *Waterworld* (1995) that bomb in the United States, the least-common-vocabulary position is plausible. Commercial directors who refuse to sacrifice speech to sight do not generally make blockbusters.¹⁴

As a result of the dumbing-down of the English language solely for profit's sake, the language suffers, and American culture suffers, as we are increasingly exposed to less and less sophisticated verbal communication. As Neil Postman asserts in his book *Amusing Ourselves to Death*, "When serious public conversation becomes a form of baby-talk, when, in short, a people become an audience and their public business a vaudeville act, then a nation finds itself at risk; culture death is a clear possibility."¹⁵

Sadly, these effects are not solely confined to the English language. As Lee Hotz of the *Los Angeles Times* keenly observes: "The world has become a hospice for dying languages, which are succumbing to the pressure of global commerce, telecommunications, tourism, and the inescapable influence of the English language. By

the most reliable estimates, more than half the world's 6500 languages may be extinct by the end of this century."¹⁶ The mass media and the Internet are responsible for spreading the English language like a virus. This process can have an enormously negative impact on other cultures.

In reality, thousands of minority languages are clinging precariously to existence. A few, like Hebrew and Gaelic, are being rejuvenated as a consequence of resurgent nationalism. The importance of language to political and personal self-determination cannot be stressed enough. A people's right to speak its mind in the language of its choice is becoming an international human right.¹⁷ By forcing English on other cultures, the US has the potential to influence the thoughts of entire nations.

A little known fact, and one conveniently omitted in American history textbooks, is that all Native American and Hawaiian languages were for a century the target of US Government policies designed to eradicate them in public and in private, replacing them with English. This was to ensure that these languages were not passed from parent to child. In fact, until 1987, it was actually illegal even to teach Hawaiian in the islands' public schools. This seems foolish considering the fact that Hawaii once claimed to have the world's highest literacy rate.¹⁸ Generations were left with no direct connection to their language or tribal cultures.

Such language control bears a stark resemblance to the enforced tyranny of language imposed by The Party in 1984. To disconnect generations was one of the goals of Newspeak:

When Oldspeak had been once and for all superceded, the last link with the past would have been severed. History had already been rewritten, but fragments of the literature survived here and there, imperfectly censored, and so long as one retained one's

knowledge of Oldspeak, it was possible to read them. In the future such fragments, even if they chanced to survive, would be unintelligible and untranslatable.¹⁹

It is curious to note that this US policy was in effect long before the year 1984, and even before 1948, which is when Orwell wrote *1984*. The depressing reality is that linguistic repression has already played a pivotal role in US history, and realistically always will.

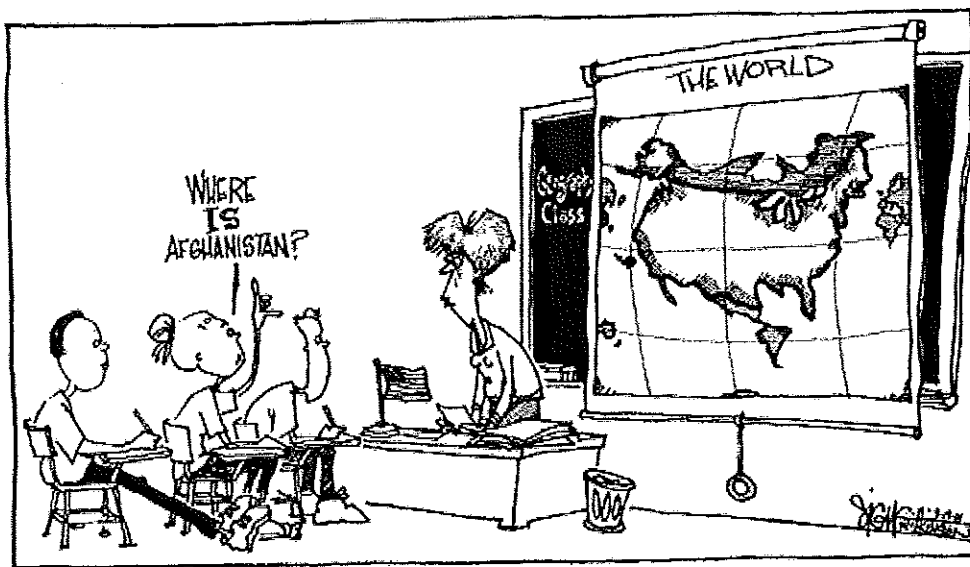
In 1868, a federal commission on Indian affairs concluded: "In the difference of language today lies two-thirds of our trouble....Their barbarous dialect should be blotted out and the English language substituted." The commission reasoned that "through sameness of language is produced sameness of sentiment, and thought....In process of time the differences producing trouble would have been gradually obliterated."²⁰

Perhaps, there is no more powerful testimony to the visceral importance of language than the nineteenth-century US government's systematic efforts to destroy all indigenous languages and replace them with English. Indeed, no language in memory, except Spanish, has sought more forcefully to colonize the mind than the English language has.

The Internet is perhaps the best evidence in existence of US linguistic imperialism. Most people do not know where the Internet came from. Most don't care, either. They probably think Microsoft invented it. In truth, the Internet was originally known as the ARPANET, which stood for the Advanced Research Projects Agency Network. ARPA was the forerunner to what is today known as DARPA, the Defense Advanced Research Projects Agency. It is a branch of the US Department of Defense that conducts research programs with primarily military applications. However, these

programs inevitably squirm their way into the private sector, labeled as “cutting-edge technology” when they do.

It can be argued that English is essentially the universal language of the Internet. The main reason is academic. Originally, the ARPANET was set up between universities with government contracts. Today, most researchers all over the world use English, and often relevant terminology is more stable and more well-known in English than in their own respective languages. To maximize the number of interested people in a project, researchers often use English, even if it is not spoken by the majority of their country’s population. More readers mean more money. Thus, the use of English in essentially national contexts continues to grow.²¹



22

None of this is shocking when one considers that the US Government invented the Internet. Why shouldn't English be its official language? Regardless, official or unofficial, it's here to stay. The Internet is *the* most powerful communication tool that any government in world history has ever had at its disposal. Thus, by increasing the importance of English, the importance of other languages is decreased.

O'Brien, an evil member of the Inner Party in *1984*, says to Winston, the novel's protagonist: "Since military and commercial rivalry are no longer important, the level of popular education is declining. What opinions the masses hold, or do not hold, is looked on as a matter of indifference. They can be granted intellectual liberty because they have no intellect."²³ Linguistic atrophy is responsible for the intellectual reduction O'Brien speaks of.

Actually, a possibility exists that our popular culture has another, more cynical, reason for existing. Ralph Waldo Emerson said it best: "If you would rule the world quietly, you must keep it amused." This concept is demonstrated in Oceania society. There, average citizens revert to a style of life that seems to be natural to them, a sort of ancestral pattern: "Heavy physical work, the care of home and children, petty quarrels with neighbors, films, football, beer, and above all, gambling [fill] up the horizon of their minds. To keep them in control [is] not difficult."²⁴

"Orwell always assumed that politics would remain a distinct, although corrupted, mode of discourse," asserts Postman. "That the defense of the indefensible would be conducted as a form of amusement did not occur to him. He feared the politician as deceiver, not as entertainer."²⁵ Maybe so, but it is also still possible that entertainment is just a smokescreen, and that oppression still remains the ultimate goal of the power elite.

Noam Chomsky, perhaps the nation's most controversial and most celebrated critic of contemporary society, adds credibility to this argument in his essay "Media Control: the Spectacular Achievements of Propaganda," when he says:

The bewildered herd is a problem. We've got to prevent their roar and trampling. We've got to distract them. They should be watching the Super Bowl or sitcoms or violent movies. Every once in a while you call on them to chant meaningless slogans

like "Support our troops." You've got to keep them pretty scared, because unless they're properly scared and frightened of all kinds of devils that are going to destroy them from outside or inside or somewhere, they may start to think, which is very dangerous, because they're not competent to think. Therefore it's important to distract them and marginalize them.²⁶

This is the concept of "manufacturing consent," which Edward Bernays, one of the leading public relations figures in the country has described "as the essence of democracy."²⁷

In the US, would-be intellectuals are subdued by the subtle and often almost imperceptible imposition of language. This imposition of thought through words by less-than-dazzling intellects is indeed elitism, an oligarchy of mediocrity that sometimes imposes rules of language implying a social agenda that most of us don't really believe in.²⁸ An example of popular culture's influence upon behavior through linguistic manipulation can be found in a simple analysis of the titles of several songs of the popular boy band NSYNC:

"For The Girl Who Has Everything"...buy this CD.
"Bye Bye Bye" – or perhaps, "Buy Buy Buy"

Another example is provided by cars. Many models end in "ZX," "SX," and "CX." These names, when pronounced, sound suspiciously like the word "sex." Car makers are selling sex.

Local Bowling Green, KY, DJ Eric Beason explains why he thinks titles are like this: "If anyone ever actually stopped to think about what these guys were actually singing, they'd realize it was garbage and would never buy it. But titles like this trick people into buying this type of music before they realize what they're doing. By the time

they do, it's too late and they've already spent the money. And you know open CD's can't be returned."²⁹

Yet, often pop music is used as a form of cultural currency between teens. Metaphors are constructed around pop music, providing teens with only one worldview, an increasingly narrower vocabulary which makes thinking easier. This linguistic trend is described as "McLanguage," by Priscilla Vail, author of *Clear and Lively Writing* and *Smart Kids with School Problems*. "It's verbal fast food made up of inflection, gesture, and condensation."³⁰

The few individuals who do know enough to question the status quo are often dismissed as pessimistic. An increasingly popular accusatory term is *paranoid*, which over the past decade, thanks to the *X-Files*, has taken on a negative, schizophrenic, almost insane connotation. It's no wonder the one thing Winston quietly reminds himself of while imprisoned in 1984 is that "sanity is not statistical."³¹ However, when one makes a man feel that he is alone in his thinking, his will can be broken, and eventually the heretical thought is abandoned for one more favorable to the societal norms perpetuated by the state and its control over the people's language.

Humans naturally shy away from mentally uncharted paths. As a result, linguistic routines psychologically inoculate people against the anxiety caused by the chaos that believing in the unknown affects people with. Thankfully, it is this fear that pop culture and the mass media rescue us all from. Richard Saul Wurman explains this in his book *Information Anxiety*. "Our language gets stifled from laziness, thoughtlessness, and well-meaning criticism from linguistic police, i.e., parents, critics, teachers, who are trying to teach us a uniform language and may be themselves threatened by its flexibility," writes

Wurman.³² As was stated at the very beginning of the chapter, those who master language are confronted with a terrifying freedom. If authority figures fear linguistic self-reflection, then why would the masses ever feel obligated, indeed even permitted, to question anything?

On speaking of mass media influence in America, Chomsky further explains: “They [men] are terrible judges of their own interests, so we have to do it for them for their own benefit. Actually, it’s very similar to Leninism. We do things for you, and we are doing it in the interest of everyone.”³³

In Oceana, technology displaces thought. It doesn’t take a leap of faith to see this in America, either. Orwell predicts this when he says: “The pen was an archaic instrument, seldom used even for signatures.”³⁴ Today, email forces people to type letters to each other more than they hand write them. Postcards aren’t mailed; they’re emailed. Over the next ten years, typing skills will be given more emphasis in the classrooms than penmanship. Taking this one step further, voice recognition software is becoming mainstream now. With this technology, who’s to say that even typing skills won’t become a lost art, displaced by a more “efficient” means of communication?

Just recently, America Online released AIM 4.7, the newest installment of its popular, and free, Instant Messenger service. In version 4.7, a new, thought-reducing tool emerged known as the *emoticon*. Emoticons are short for emotional-icons. These are the little yellow-painted faces that the user can select to symbolize any number of emotions. AIM users can now have an entirely visual, mentally effortless conversation with someone just by pointing and clicking, without ever having to type a single word or think of its consequences ☹. Postman adds that “the substitution of immediate, pictorial

material for the written word may be destroying our societal ability to reason intelligently.”³⁵

Oceana even has novel writing machines. In the end, “books were just a commodity that had to be produced, like jam or bootlaces.”³⁶ Does the technology exist for a computer to write a novel so convincing that it can trick someone into believing that it was written by another human being? Even if it not, doesn’t it sometimes feel as though much of our pop culture *is* manufactured, to the point of absurdity?

This is disturbing, because the ability, and yes the desire, for free thinking, decreases as humans are given fewer and fewer ways to express themselves. Technology simplifies the mind, reduces the perceived available vocabulary in the English language, and, thus, thought complexity. Apparently verbal skills follow the old cliché that “if you don’t use it, you lose it.” Indeed, as Winston began his diary, “it was curious that he seemed not merely to have lost the power of expressing himself, but even to have forgotten what it was that he had originally intended to say.”³⁷ If one can’t label a thought, then it can’t be remembered, and it certainly can’t be written down. It evaporates.

Howard Bloom, in his keynote address to the massive compendium *Disinformation: You Are being Lied To*, from an excerpt in his own book *Global Brain: The Evolution of Mass Mind from the Big Bang to the 21st Century*, suggests that reality is a shared hallucination. He asserts that “individual perception untainted by others’ influence does not exist.”³⁸

As in the case of Big Brother in 1984, if all the records told the same tale, then the lie passed into history and became truth. “Who controls the past,” ran the Party slogan,

“controls the future: who controls the present controls the past.” All that was needed was an unending series of victories over memory. This was otherwise known as “reality control,” or in Newspeak, the official language of Oceania, “Doublethink.”³⁹

Taking this one step further, O’Brien teaches Winston about reality:

O’Brien: “Then where does the past exist, if at all?”

Winston: “In records, it is written down.”

O’Brien: “In records. And-?”

Winston: “In the mind. In human memories.”

O’Brien: “In memory. Very well, then. We, the Party, control all records, and we control all memories. Then we control the past, do we not?...But, I tell you, Winston, that reality is not external. Reality exists in the human mind, and nowhere else.”⁴⁰

Orwell goes on to argue that if this is true, “how could the immortal, collective brain be mistaken? By what external standards could you check its judgments?”⁴¹ Howard Bloom echoes this concept more than a half century later when he says that “memory is the core of what we call reality.”⁴²

In the late 1970’s one of the world’s most preeminent memory researchers, Elizabeth Loftus, performed a series of key experiments. In one such experiment, test subjects were shown a small video clip of a collision between a bicycle and an auto driven by a brunette. Afterwards they were inundated with questions about the “blond” behind the steering wheel. Not only did all the test subjects remember the nonexistent blond, but once they viewed the clip again, had a hard time believing that it was even the same clip.

One test subject said: “It’s really strange because I still have the blonde girl’s face in my mind and it doesn’t correspond to her [pointing to the woman on the video screen]...It was really weird.” Regarding memory, Loftus concluded that information

leaked to us by fellow humans overrides the scene we're sure we've just "seen with our own eyes."⁴³ This innate weakness of ours puts us at the mercy of a conformity enforcer whose power and subtlety are almost beyond belief.

Ultimately, it comes down to language. Bloom captures the essence of our linguistic fate as a society when he reveals that

The ultimate repository of herd influence is language- a device which not only condenses the opinions of those with whom we share a common vocabulary, but sums up the perceptual approach of swarms who have passed on. Every word we use carries with it the experience of generation after generation of men, women, families, tribes, and nations, often including their insights, value judgments, ignorance, and spiritual beliefs.⁴⁴

Essentially, humans are at the mercy of their ancestors. Their perceptual influence is almost unimaginable.

The experiences that physiologist/ ornithologist Jared Diamond had while in New Guinea demonstrate the powerful influence vocabulary, and ultimately language, has on humans. Diamond was in New Guinea trying to study the various bird species he found. He used the knowledge he gained in zoology classes he attended back in the US. Diamond used binoculars and what he believed to be state-of-the-art taxonomy. To his dismay, despite all his supposed superior knowledge, Diamond was only laughed at by the New Guineans, who were bestowed with a far more reaching vocabulary, each word of which compacted the experiences of armies of bird-hunting ancestors before them.⁴⁵ The simple truth is that their vocabulary was better suited to the task of bird taxonomy than Diamond's was, contrary to what Diamond had expected to find. Whorf further explains this concept:

The American Indian language Hopi offers an interesting example of the relationship between thought and language

and the understanding of things around us. In Hopi, events are always referenced to space and time by two tenses (objective and subjective) and, thus, function without the need for our tenses (past, present, future, etc.) or, for that matter, any reference to time. To think or speak in Hopi (or any language) is to accept the structure of thinking inherent in that language. How you think affects how you deal with information and how you use it.⁴⁶

On a final note, the stored experience language carries can make the difference between life and death. For roughly 4000 years, Tasmanian families starved to death when famine struck, despite the fact that their island home was surrounded by fish-rich seas. They died simply because their tribal culture did not define fish as food.⁴⁷

Extrapolating this one step further into present-day society, food can be substituted with knowledge and truth. If society doesn't define "X" as a way to solve a problem, then people won't turn to it for their answer. Thus, even though American citizens are all free to seek alternative sources of information, because their popular culture tells them that they only need to watch CNN, for example, for all of their informational needs, then accordingly, they won't feel the need to look elsewhere. Should a discrepancy arise, CNN can always say that the public could have always verified its information elsewhere, if it were *so* concerned.

All too often when we see someone perform an action without a name, we rapidly forget its alien outlines and tailor our recall to fit the patterns dictated by convention...and conventional vocabulary.⁴⁸ This segues into the most important linguistic aspect of *1984*: the Newspeak Dictionary.

Newspeak is the official language of Oceania. It's influence is so vital to Oceanic society and the perpetuation of The Party and Big Brother, the personification of The Party, that Orwell devotes an entire Appendix to it in *1984*, entitled "The Principles of

Newspeak.” Orwell expected that Newspeak would have finally superceded Oldspeak (standard English) by about 2050. This date is almost a half century away. The possibility still exists, and will for quite some time, that in 2050 an American-English derivative of Newspeak will be the official language of the United States, and quite possibly the rest of the world, whatever it may look like by then. According to Orwell:

The purpose of Newspeak was not only to provide a medium of expression for the world-view and mental habits proper to the devotees of Ingsoc, but to make all other modes of thought impossible...Newspeak was designed not to extend but to *diminish* the range of thought, and this purpose was indirectly assisted by cutting the choice of words down to a minimum.⁴⁹

In present-day America, for example, the decreased awareness that accompanies a decrease in thought is essential to the public mindset in our so-called “War on Terrorism.” For victory, a “mentality appropriate to a state of war” should exist.⁵⁰ The metaphor that *argument is war* is also vital to this US mentality. This battle we’re in, though no side will diplomatically admit to it, is more theological and ideological than anything else. We only use force when our words fail us. Fortunately, our language provides a suitable breeding ground for this type of thought. The following examination by George Lakoff in his book *Metaphors We Live By* reveals this to be the case:

ARGUMENT IS WAR

Your claims are *indefensible*.
He *attacked every weak point* in my argument.
His criticisms were *right on target*.
I *demolished* his argument.
I’ve never *won* an argument with him.
You disagree? Okay, *shoot!*
If you use that *strategy*, he’ll *wipe you out*.
He *shot down* all of my arguments.

Many of the things we *do* in arguing are partially structured by the concept of war. Though there is no physical battle, there is a verbal battle, and the structure of an argument-- attack, defense, counterattack, etc.-- reflects this. It is in this sense that the ARGUMENT IS WAR metaphor is one that we live by in this culture; it structures the actions we perform in arguing.⁵¹ This sort of language facilitates the war effort.

Joshua Meyrowitz expands upon this in his ground-breaking book entitled *No Sense of Place*, which explores the impact of electronic media on social behavior. Meyrowitz points out that “our actions are always ‘defensive,’ theirs are always ‘aggressive.’ Our interventions are ‘rescue missions to preserve Freedom’; theirs are ‘invasions to crush the will of the people.’ Our economic assistance to underdeveloped countries is ‘humanitarian’; theirs is ‘propagandistic.’ Mind-boggling weapons of death are benignly labeled as ‘peacekeepers,’ while many would-be peacekeepers are surrounded by hints of treason.”⁵²

Going back in history, one realizes that this type of language has always been with us. FDR coined the phrase “lend-lease” as a way to provide weapons to beleaguered England at a time during WWII when the US was diplomatically neutral and actively helping England was banned. “Social Security” was a clever name for government – provided pension. Recessions were known as “rolling readjustments” under Eisenhower. Edward Kennedy mocked Reagan’s Strategic Defense Initiative by renaming it “Star Wars,” a pop culture name from the hit movie series, which is what most Americans know the program as today, if they even know it exists. Today, President Bush doesn’t talk about funneling money to religious groups to provide help for the poor. Instead, he talks about providing federal aid to “faith-based institutions” to assist those in need.⁵³

Regarding Oceanic citizens, Orwell notes: "All that was required of them was a primitive patriotism which could be appealed to whenever it was necessary to make them accept longer working hours or shorter rations. And even when they became discontented, their discontent led nowhere, because, being without general ideas, they could only focus it on petty specific grievances. The larger evils invariably escaped their notice."⁵⁴



Oceanic citizens' lack of language reduced their potential for thought, and thus awareness. Indeed, to facilitate this, the Newspeak Dictionary had *The B Vocabulary*:

The B vocabulary consisted of words which had been deliberately constructed for political purposes: words, that is to say, which not only had in every case a political implication, but were intended to impose a desirable mental attitude upon the person using them... The B words were a sort of verbal shorthand, often packing whole ideas into a few syllables, and at the same time more accurate and forcible than ordinary language... It was perceived that in thus abbreviating a name one narrowed and subtly altered its meaning, by cutting out most of the associations that would otherwise cling to it.⁵⁶

Orwell gives the example of the *Communist International* in the former USSR, which was shortened to *Comintern*. It is a word that can almost be uttered without thought, whereas *Communist International* is a phrase which the mind might tend to momentarily linger upon. In the US the same can be said for the *Federal Bureau of Investigation*, the *Central Intelligence Agency*, and the *Internal Revenue Service*. FBI, CIA, and IRS are words that are more easily pronounceable, and, more importantly, words that are easily said without much thought and mentally dismissed just as quickly without conjuring up feelings of hatred and distrust. As a side note, Americans curiously no longer have a desire for Kentucky Fried Chicken, but they do want some KFC ☺

Perhaps, Syme, a minor but unusually insightful character whose only job is the construction of the Eleventh Edition of the Newspeak dictionary, explains the goal of Newspeak best in a conversation he has with Winston:

Don't you see that the whole aim of Newspeak is to narrow the range of thought? Every concept that can ever be needed will be expressed by exactly *one* word, with its meaning rigidly defined and all its subsidiary meanings rubbed out and forgotten. Every year fewer and fewer words, and the range of consciousness always a little smaller...It's a beautiful thing, the destruction of words.⁵⁷

Each reduction is actually a gain so far as The Party is concerned. Therefore, the smaller the area of choice, the smaller the temptation to take thought.

If the US Government controls the language people use through the mass media, it will have an easier time controlling people's thoughts as well. Ultimately, unorthodox thinking becomes almost impossible if all people speak the same language, with their words chosen from the same dictionary. The potential then exists for the government to calculate all of the possibilities, and probabilities, of having a certain, single thought,

given a fixed stimulus, if all citizens choose their words, and therefore thoughts, from the same source. It doesn't get any prettier than that. In fact, in a 1977 *Rolling Stone* article, Watergate muckraker Carl Bernstein uncovered a list of over 400 reporters and a coterie of publishers and media moguls who had basically been rubber-stamping CIA propaganda since the 1950s. The group included *Life* and *Time* magazine's Henry Luce, CBS's William Paley, and *New York Times* publisher Arthur Hays Sulzberger. One CIA official anonymously admitted that "one journalist is worth 20 agents."⁵⁸ Additionally, during the Kosovo conflict, it was uncovered that CNN had hired five "interns" who were actually US Army Intelligence employees. A US Army spokesman was quoted as saying, "Psyops personnel, soldiers and officers, have been working in CNN's headquarters in Atlanta through our program 'Training with Industry.'"⁵⁹

The intriguing possibility exists that the media elite have even found a linguistic biorhythm inherent in American-English. Language is math and math is language. Math has patterns and so does language. Rhythm is mathematically reducible. Music is rhythm. It is widely known that music can hypnotize. Our cultural engineers may be tapping into a publicly uncharted biorhythm in the American-English language that subconsciously is hypnotizing audiences with its linguistic patterns. Audiences like this hypnotic, tension-reducing sensation in their brains, but aren't even aware of it. Instead, they see an image and grab hold of it as if it were a life-saving log floating by, saving them from drowning in a river of mental chaos. In our visually dominated culture, this image becomes their reason for loving what they see and hear, and not the hidden pattern. They don't love the language so much as they love the rhythm in their head. Conveniently, these rhythmic echoes are annoyingly difficult to forget. *The media elite have found a way to make the*

alphabet dance and audiences love watching. Oceanic society reflects this possibility, in that the ultimate goal of Newspeak is to “consciously induce unconsciousness, and then, once again, to become unconscious of the act of hypnosis you had just performed.”⁶⁰

The Simpsons TV show on the FOX network provides a perfect modern illustration of this concept. In the episode titled “New Kids on the Bleccch,” Bart gets in hot water when he cheats his way to first place in a Springfield marathon. He’s rescued from the angry mob by LT Smash, a boy band music producer who wants to turn Bart and his friends Millhouse, Nelson, and Ralph Wiggum into the next new pop sensation as the “Party Posse.” Their hit song is titled “Yvan Eht Nioj,” which they curiously perform on a US aircraft carrier.

These are the lyrics, “Oh, say can you rock! There’s trouble in a far off nation. Time to get in love formation. Your love is more deadly than Sadaam. That’s why I gotta drop the bomb! Yvan Eht Nioj (chorus)....” Lisa hears Homer chanting the chorus line “Yvan Eht Nioj” over and over again. When she asks him what it means, he says “it doesn’t mean anything. Like ramalama ding dong, or give peace a chance.” Then she realizes that “Yvan Eht Nioj” is really “Join the Navy” spelled backwards. She plays the video in slow motion to reveal a subliminal photo of an “Uncle Sam” poster. When Lisa confronts L.T. Smash, she finds his name is really Lt. Smash, or Lieutenant Smash, and that he’s a US Naval Recruiting Officer. Smash goes on to explain that “it’s a three-pronged attack. Subliminal, liminal, and super liminal.” Lisa quips, “Super liminal?” Smash replies, “I’ll show you...HEY YOU! Join the Navy!” Then the scene cuts out to a shot of two of Homer’s friends, Carl and Lenny, who reply, “Yeah, alright,” and “I’m in,” respectively.⁶¹

Ultimately, it is conceivable that by the time 2050 finally does roll around, the mass media will have had enough time to transform the English language of today into a derivative of Newspeak and without the average citizen ever being aware of the change until it's too late... if he or she ever notices it in the first place.

Endnotes

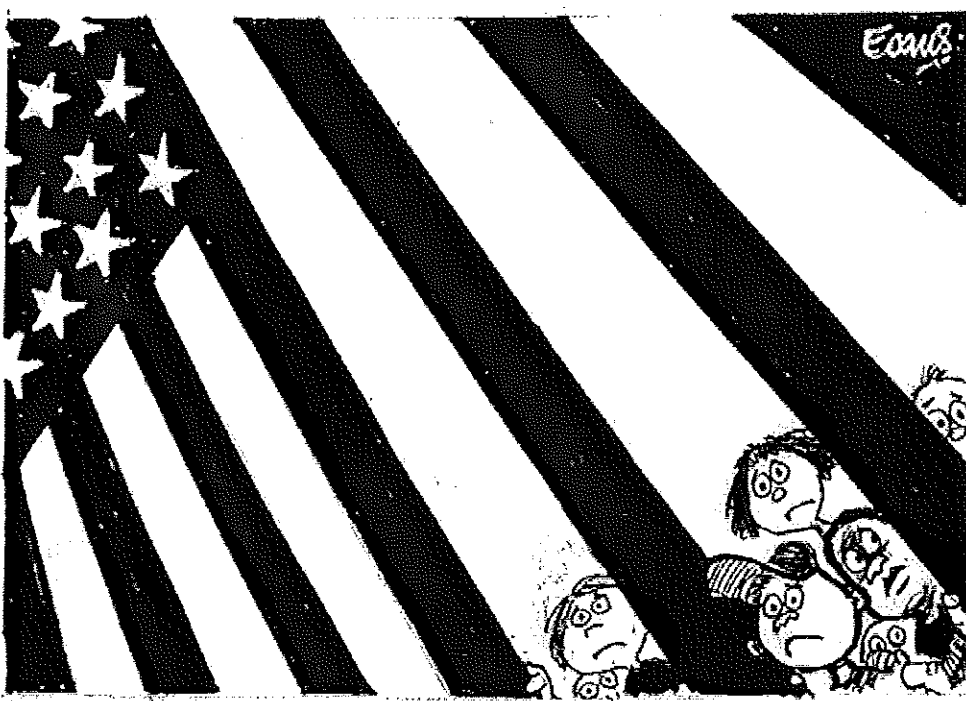
- ¹ George Orwell, "Politics and the English Language." (1946), <http://www.assumption.edu/dept/history/His130/PoliticsAndLanguage.html>.
- ² Dan Slobin, "Language and Thought." (U of California at Berkely, 1996), <http://ihd.berkeley.edu/slobin.htm>.
- ³ George Orwell, 1984 (New York: Signet Classic, 1950), 24.
- ⁴ Daryl Cagle, home page, <http://cagle.slate.msn.com>.
- ⁵ Orwell, 1.
- ⁶ E. Zigler and Frank M., The Parental Leave Crisis (New Haven: Yale University Press, 1988).
- ⁷ Jane M Healey, Endangered Minds (New York: Touchstone, 1999), 22.
- ⁸ *Ibid.*, 18.
- ⁹ Orwell, 6.
- ¹⁰ Daniel Goleman, "Infants Under 2 Seem to Learn From TV," New York Times, 22 Nov. 1988.
- ¹¹ Healey, 85.
- ¹² Bernice Cullinan, Children's Literature in the Reading Program (Newark, DE: IRA, 1987).
- ¹³ Healey, 37.
- ¹⁴ Todd Gitlin, Media Unlimited (New York: Metropolitan Books, 2001), 94.
- ¹⁵ Neil Postman, Amusing Ourselves to Death (New York, Penguin Books Ltd., 1985), 155-156.
- ¹⁶ Lee Hotz, "The Impassioned Fight to Save Dying Languages," LA Times Online, 2000.
- ¹⁷ *Ibid.*, 2.
- ¹⁸ *Ibid.*, 2.
- ¹⁹ Orwell, 255.
- ²⁰ Jukka Korpela, "English, the Universal Language on the Internet?" Home page. <http://www.cs.tut.fi/~jkorpela/lingua-franca.html>.
- ²¹ *Ibid.*, 2
- ²² Daryl Cagle, home page, <http://cagle.slate.msn.com/>.
- ²³ Orwell, 173.
- ²⁴ *Ibid.*, 61-62.
- ²⁵ Postman, 129.
- ²⁶ Noam Chomsky, Media Control: the Spectacular Achievements of Propaganda, (Canada: Seven Stories Press, 1997) 22-23.
- ²⁷ *Ibid.*, 24.
- ²⁸ Angela Shanahan, "Language in Moral Straights," The Australian, 27 Nov. 2001.
- ²⁹ Eric Beason, interview by author, Bowling Green, KY, 27 April 2002.
- ³⁰ Priscilla Vail, Smart Kids with School Problems (New York: NAL, 1989).
- ³¹ Orwell, 179.
- ³² Richard Saul Wurman, Information Anxiety (New York: Double Day, 1989), 111.
- ³³ Noam Chomsky, "What Makes the Mainstream Media Mainstream" (Z Media Institute, June 1997).
- ³⁴ Orwell, 9.
- ³⁵ Postman, 112.
- ³⁶ Orwell, 108.

-
- ³⁷ Ibid., 10.
- ³⁸ Russ Kick, Disinformation: You Are Being Lied To (China: The Disinformation Company, 2002), 12.
- ³⁹ Orwell, 32.
- ⁴⁰ Ibid., 205.
- ⁴¹ Ibid., 228.
- ⁴² Howard Bloom, "Reality Is A Shared Hallucination," in Global Brain: The Evolution of Mass Mind from the Big Bang to the 21st Century, ed. Russ Kick (China: The Disinformation Company, 2002), 12.
- ⁴³ Elizabeth Loftus, Memory: Surprising New Insights Into How We Remember and Why We Forget, (Reading, MA: Addison Wesley, 1980), 45-49.
- ⁴⁴ Bloom, 15.
- ⁴⁵ Jared Diamond, "The Fellow Frog, Name Belong-Him Dakwo," Natural History, April 1989: 16-23.
- ⁴⁶ Wurman, 105.
- ⁴⁷ Daniel J Boorstin, The Discoverers: A History of Man's Search to Know His World and Himself (New York: Vintage Books, 1985), 344-357.
- ⁴⁸ Peter N Stearns, "The Rise of Sibling Jealousy in the Twentieth Century," in Emotion and Social Change: Toward a New Psychohistory (New York: Holmes & Meier, 1988), 197-209.
- ⁴⁹ Orwell, 246-247.
- ⁵⁰ Ibid., 158.
- ⁵¹ George Lakoff, Metaphors We Live By (Chicago: University of Chicago Press, 1981), 4.
- ⁵² Joshua Meyrowitz, No Sense of Place (New York: Oxford University Press, 1985), 321.
- ⁵³ Will Lester, "Reinvention of Language Thrives," Associated Press, 2 Feb. 2001.
- ⁵⁴ Orwell, 62.
- ⁵⁵ Daryl Cagle, home page, <http://cagle.slate.msn.com/>.
- ⁵⁶ Ibid., 249, 253.
- ⁵⁷ Ibid., 45-46.
- ⁵⁸ Greg Bishop, "The Covert News Network" in Disinformation: You Are Being Lied To ed. Russ Kick (China: The Disinformation Company Ltd, 2002), 41.
- ⁵⁹ Ibid., 42.
- ⁶⁰ Orwell, 33.
- ⁶¹ Kidzworld, "The Simpsons—New Kids on the Bleccch," 25 Feb. 2001
<http://www.kidzworld.com/site/p461.htm>.

Big Brother Is Watching You

"You already have zero privacy. Get over it."
-Scott McNealy, CEO Sun Microsystems, 1999

"They that can give up essential liberty to obtain safety deserve neither liberty nor safety."
-Benjamin Franklin, 1759



The concept of "Big Brother" is the only term from 1984 with street recognition. It is perhaps Orwell's greatest contribution to present-day American society. Today, Big Brother is synonymous with a surveillance state. To most, Big Brother also means the U.S Government. Since the September 11th Attacks, Big Brother is a term being used

more and more by the news media, which in turn slowly acclimate the public to the concept and the worldview it suggests.

Orwell accurately predicted the rise of the surveillance state. Even though America is thankfully not totalitarian like Oceania yet, it is authoritarian, and whatever gaps there are between the two can be easily closed with current technology, a frightening, yet realistic thought. It is these sociological gaps that still provide a glimmer of hope, no matter how small.

It is ironic to note that the world's first, practical, commercially available personal computer, the Apple Macintosh, arrived in 1984. Apple suitably had a *1984* theme in its ad campaign. The slogan was that the Macintosh could provide people with intellectual freedom, "so that 1984 won't be like *1984*."²

Orwell predicted computerized records. There is one scene in the beginning of the novel when Winston is at the Ministry of Truth where he "dialed 'back numbers' on the telescreen and called for the appropriate issues of the *Times*, which slid out of the pneumatic tube after only a few minutes delay."³ This equates to an Oceanic Internet.

One unsettling notion with regard to computerized records is found during a scene inside the Ministry of Truth, where Winston works in the records department. In this scene, Winston is forced to "rewrite a paragraph of Big Brother's speech in such a way as to make him predict the thing that actually happened."⁴ Basically, his task is to rewrite history, in a way favorable to The Party. The ominous implications for modern-day society's history being rewritten by the intelligence agencies of the world when various archives are declassified are overwhelming, yet not all that surprising. Who is to say that when much of the KGB's cold war archives were finally released to the public, that what

those files contained was absolute truth? In fact, it is a real possibility that the real truth may never be known about the farthest extent of the atrocities committed by the communist regimes in Russia and the Soviet Union.

The same goes for China, only they're much worse, because no discrediting information is ever released by its government. It's not hard to believe that if the Chinese government ever does release intelligence archives about "what really happened" that they won't completely rewrite Chinese history in a way that makes the current regime look virtuous while blaming any atrocities on past regimes.

The same also goes for America. Hundreds of books have been written about the abuses of the 13 members of the US Intelligence Community: the Central Intelligence Agency; Defense Intelligence Agency; National Security Agency; Army, Air Force, Navy and Marine Corps Intelligence; National Imagery and Mapping Agency, National Reconnaissance Office, Federal Bureau of Investigation, Department of Treasury, Department of Energy, and the Department of State.⁵ The new Office of Homeland security has not yet been classified as the fourteenth member, as of this writing, although, it, much like the CIA, coordinates all of its intelligence activities with all of the other Intelligence Community members.

All may not be lost, according Joshua Meyrowitz, who points out that "The simple mathematics of hierarchy suggests the stronger likelihood of an undermining of the pyramid status in an electronic age." He goes on to suggest that the telephone and computer provide a "horizontal flow of information" that should be a "deterrent to totalitarian central leadership."⁶ On the surface, this seems positively plausible, but this argument is actually counterintuitive. When Meyrowitz wrote his book in 1985, the

Internet boom had not occurred, the *X-Files* had not been produced yet. The general public's concept of the farthest reaches and capabilities of our nation's current technology was anecdotal at best. Nobody imagined the world we live in today.

Fifteen years later, we now live in a world between the "connected" vs. the "disconnected." Jeremy Rifkin, in his ground-breaking book *The Age of Access*, provides a social definition for our world that is remarkable in its clarity:

The separation of humanity into two different spheres of existence- the so-called digital divide- represents a defining moment in history. When one segment of the human population is no longer able to communicate with the other in terms of time and space, the question of access takes on a political import of historic proportions.⁷

The advent of the personal computer has given governments more power to keep their populations under surveillance and control than ever before. The telescreen is Orwell's *1984* equivalent of today's personal computer. An interesting quote which hints at this possibility comes from a conversation between Winston Smith and Mr. Charrington, an old man who owns a store and later rents the room above it to a privacy-seeking Winston. Upon entering the store, Winston cannot help murmuring: "There's no telescreen!"

"Ah," says the old man, "I never had one of those things. Too expensive. And I never seemed to feel the need of it, somehow."⁸

Could this be the personal computer of today? The language the old man uses strangely echoes that of many elderly citizens today when asked why they never bought a computer. In *1984*, telescreens told citizens what time it was, gave them biofeedback, provided them with information and news of all degrees, and kept them under total audio and video surveillance.

Today, web cams can be programmed to keep an eye on people using their own computers against them. Couldn't these web cams be set up to take intermittent snapshots of people in their homes? What about spyware? This is software that logs every web site a user visits, every email sent, and every key punched. One's thoughts can easily be determined if installing a government version of this software becomes mandatory on national security grounds.

What about biometric devices in computers? Will they be made mandatory? If so, couldn't these feasibly be used to track online activity as well? Who's to say that as terrorism worsens throughout the world that at some point in the near future, citizens won't be required to use a biometric device just to use their personal computers, or even the Internet for that matter, if it is declared that the Internet played a key role in carrying out a terrorist operation? Isn't the Internet a public place?

What about broadband? Within five years, most homes in America will have broadband technology, an always-on connection to the Internet. Eventually, every facet of our existences will depend on the Internet, too. The invasion of privacy that computers make possible has been the subject of dozens of books.

Case in point, Kroger supermarkets are now testing the SecureTouch-n-Pay from the Biometric Access Corporation. A Shopper fills out a form which links a personal file to his or her unique fingerprint photo. When checking out, shoppers pay with their prints.⁹ Privacy watchdogs already had concerns about the information collected from the Kroger Plus Card. Now they're obviously even more concerned than before.

In fact, within the next decade, the advent of grid computing will make computing power just another utility that people have delivered to their homes, and an even easier

way to track citizens in any country. Grid users will experience the Internet as a seamless computational universe. And thanks to the wireless revolution, “micronodes” will be everywhere. According to Larry Smarr, director of the California Institute for Telecommunications and Informational Technology, “Because of the miniaturization of components, we’ll have billions of endpoints that are sensors, actuators and embedded processors. They’ll be in everything, monitoring stress in bridges, monitoring the environment-- ultimately, they’ll even be in our bodies, monitoring our hearts.”¹⁰



Today, GPS is used to track parolees, and has been for quite some time. Parolee systems can be programmed to alert authorities if the offender strays into a designated

off-limits area, such as a school or victim's home.¹² In fact, microchip implants are already being experimented with. Applied Digital Solutions' new "VeriChip" is another sign that September 11th has catapulted the science of security into a realm with uncharted possibilities-- and also new fears for privacy.¹³ This chip would cost about \$200, is about the size of a grain of rice, needs no internal power supply, would be difficult to remove, and is tough to mimic. It would allow the storage of very sensitive personal information, and the chip's GPS transceiver makes satellite tracking possible.

There is even a wristband version designed by Wherify for small children to allow parents to track the movements of their children with a real-time online map. An adult version will be released in the summer of 2002. According to Wherify president Timothy Neher, "This technology is going to change the way people feel about stealing kids and raping women on bike paths," he said. "It's really going to make people feel safer."¹⁴

However, Marc Prioleau, the director of marketing for SiRF whose GPS chipset is integrated into the Wherify personal locator, points out that "the overriding issue is do you create a bigger danger to the person than existed in the first place?"¹⁵ Only time will tell. Theologian and author Terry Cook said he worries the identification chip could be the "mark of the beast," an identifying mark that all people will be forced to wear just before the end times, according to the Bible.¹⁶



17

This chip may eventually be required of all Americans. Privacy advocates will undoubtedly fight legislation of this sort to the death. However, if the US Government determines that a permanent method is needed to identify people who are "safe," then these chips may indeed become the norm, perhaps even being injected surreptitiously with routine vaccinations. At first, big incentives may be offered from airlines and the government, for example, as a way to identify trusted travelers who have submitted to an FBI background check. However, eventually it is conceivable that this trusted traveler concept may be extended to include one's needing this chip to gain access to *any* general public area, government or otherwise.

In response to the September 11th tragedy, Applied Digital Solutions CEO Richard Sullivan wants to take chip tracking even one step further: "Implant all

foreigners passing through customs or immigrations with the chips,” says Sullivan. “The implanted chip would replace green cards, allowing officials to monitor their activities better and keep terrorists out. In the wake of September 11th, the government is more prepared, for the overall benefit of our citizens, to advocate some of these changes.”¹⁸

The catalyst needed for such legislation would probably be a nuclear explosion on US soil. Orwell casually hints at this being the cause for the rise of Big Brother when Winston is trying to figure out when Big Brother came into existence: “Perhaps it was the time when the atomic bomb had fallen on Colchester.”¹⁹ Dr. Frank Gaffney of the Center for Security Policy confirms this when he says, “I can tell you that if we have a weapon of mass destruction used against a major population center in this country, civil liberties are going to go by the board en masse.”²⁰



21

The USA Patriot Act, passed into law on October 26, 2001, came dangerously close to ushering in the era of an American totalitarian state. It's surprising how many supposedly educated college students aren't even aware the act exists. According to Laura W. Murphy, Director of the ACLU's Washington National Office, "The USA Patriot Act gives law enforcement agencies nationwide extraordinary new powers unchecked by meaningful judicial review."²² The most troubling provisions according to the ACLU are as follows:

- Allow for indefinite detention of non-citizens who are not terrorists on minor visa violations if they cannot be deported because they are stateless, their country of origin refuses to accept them or because they would face torture in their country of origin.
- Minimize judicial supervision of federal telephone and Internet surveillance by law enforcement authorities.
- Expand the ability of the government to conduct secret searches (sneak-and-peek provision)
- Give the Attorney General and the Secretary of State the power to designate domestic groups as terrorist organizations and deport any non-citizen who belongs to them.
- Grant the FBI broad access to sensitive business records about private individuals without having to show evidence of a crime.
- Lead to large-scale investigations of American citizens for "intelligence" purposes.²³

In some cases, the USA Patriot Act will fulfill the Administration's goal of being able to indefinitely imprison someone who has never been convicted of a crime. Further, it is apparent that this act will also ensnare innocent people based on their political beliefs and associations. The role of judges is minimized. The government can use its intelligence-gathering power to circumvent the standard that must be met for criminal

wiretaps (no probable cause), thus authorizing unconstitutional physical searches and wiretaps. The act permits the sharing of sensitive grand jury and wiretap information without judicial review or any safeguards regarding the future use or dissemination of such information. College students' sensitive data is no longer safe, as the USA Patriot Act gives government agents the right to receive student data collected for the purpose of statistical research under the National Education Statistics Act, without students' consent. Actually, students are powerless to stop it. The CIA director now has the power to identify domestic intelligence requirements, a power which violates its original charter. The danger exists that protestors may now be transformed into "terrorists" if they engage in conduct that "involves acts dangerous to human life."²⁴

Jon B. Utley, the Robert A. Taft fellow in constitutional and international studies at the Ludwig von Mises Institute, has a particularly insightful and timely observation, "We should think always that every new law may be enforced by our worst enemies. Think about maybe a Hilary Clinton enforcing these laws to 'investigate' conservatives."²⁵

Echoing this sentiment is US Senator Russ Feingold, D-Wisconsin, the only senator to oppose the bill. He said:

The American people will lose that war without firing a shot if we sacrifice the liberties of the American people. It is one thing to shortcut the legislative process in order to get federal financial aid to the cities hit by terrorism. We did that, and no one complained that we moved too quickly. It is quite another to press for the enactment of sweeping new powers for law enforcement that directly affect the civil liberties of the American people without due deliberation by the people's elected representatives... The Founders of our constitution did not live in comfortable and easy times of hypothetical enemies. They wrote a Constitution of limited powers and an explicit Bill of Rights to protect liberty in times of war, as well as in times of peace.²⁶

Paul Weyrich of the Free Congress Foundation continues this line of thought, “The truth is that if we further emasculate our Constitution, the terrorists will have achieved the greatest victory imaginable. Their triumph won’t just be the thousands of people they killed; the triumph will be if they see our democratic institutions crumble.”²⁷

There is even a version of this bill designed for states, known as the “Model State Emergency Health Powers Act,” a bill that 34 states are considering, and a bill that critics contend gives state governors unprecedented authority in the event of a terrorist attack or other threat to the public health.²⁸ The bill, if adopted, grants governors the power to order the collection of all data and records on citizens, ban firearms, take control of private property and quarantine entire cities. The model bill states that a public health emergency is defined as

An occurrence or imminent threat of an illness or health condition, caused by bioterrorism, epidemic or pandemic disease, or novel and highly fatal infectious agent or biological toxin, that poses a substantial risk of a significant number of human fatalities or incidents of permanent or long-term disability. Such illness or health condition includes, but is not limited to, an illness or health condition resulting from a national disaster.²⁹

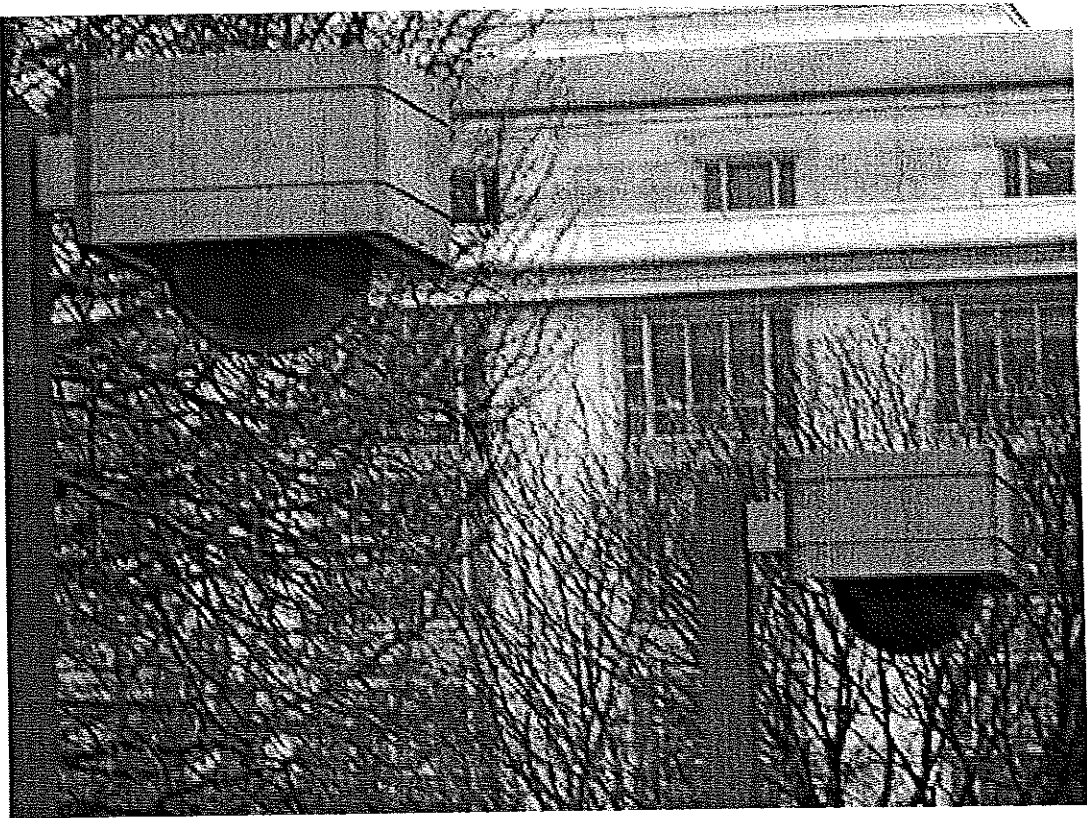
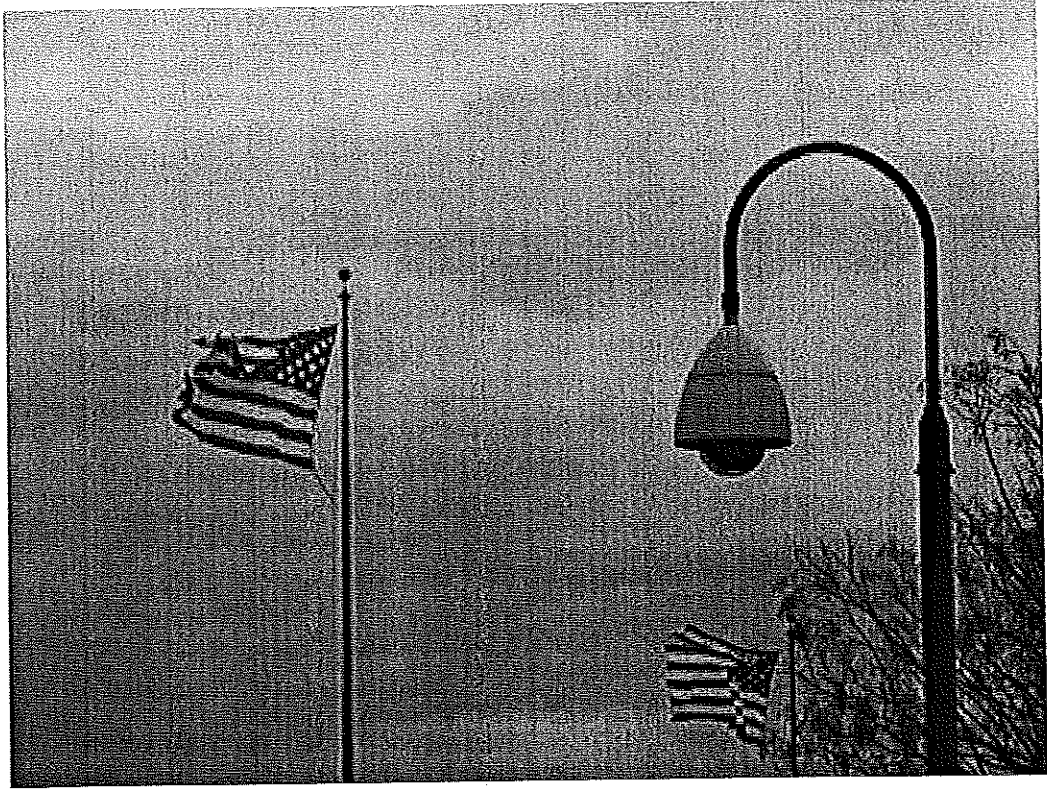
The bill’s authors defend it, saying that it is a necessary tool that gives states authority to deal rapidly with unconventional public threats. The American Legislative Exchange Council disagrees, saying that “the bill strips individuals and families of their rights and liberties at the expense of government,” while representing “unnecessary and duplicative legislation given existing state natural-disaster statutes.”³⁰

Immediately after September 11th, the US government set up inconspicuous surveillance cameras all over Washington, DC. This concept is not new. London, the actual setting of 1984, has had it for years. However, to Americans, it is a shocking and

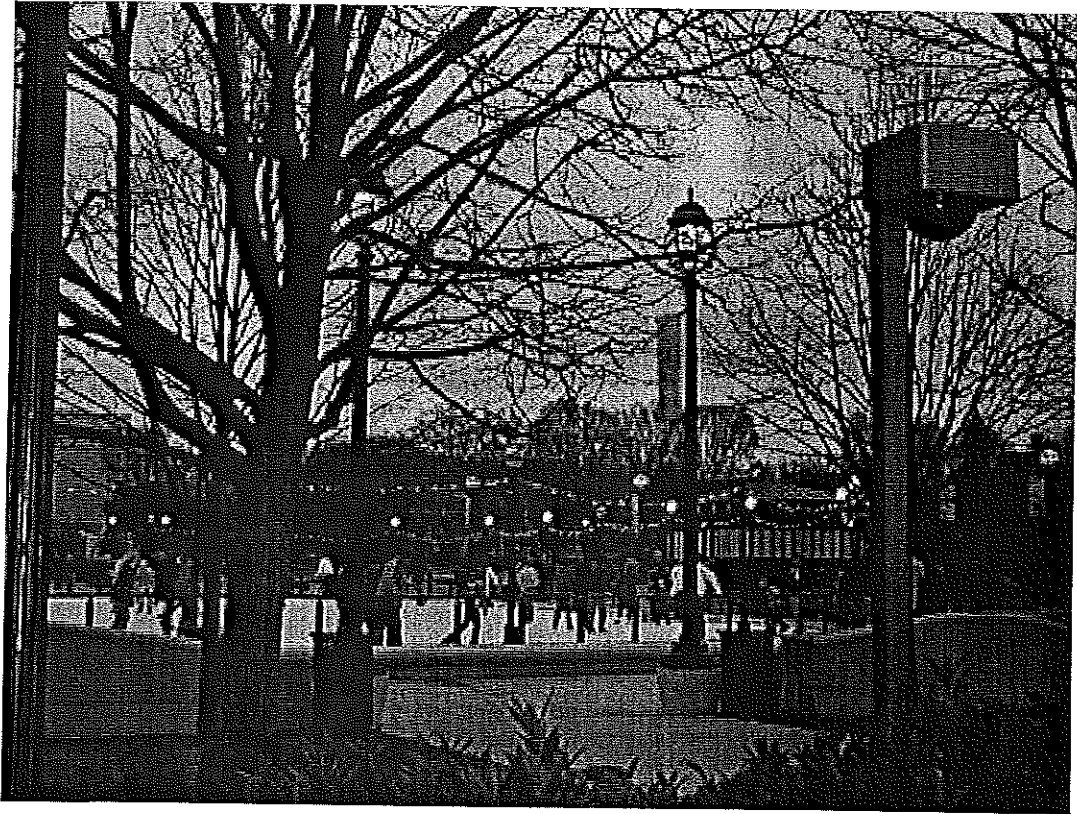
frightening sight. It is ironic to think that while these cameras make us arguably safe from other governments, they make us more vulnerable to the potential abuses of our own. This will be the trend as more and more Cold War technology is unleashed on the general public, on national security grounds.

Below are some images of these new cameras and their locations in our nation's capitol. These images are provided courtesy of EPIC, the Electronic Privacy Information Center.³¹

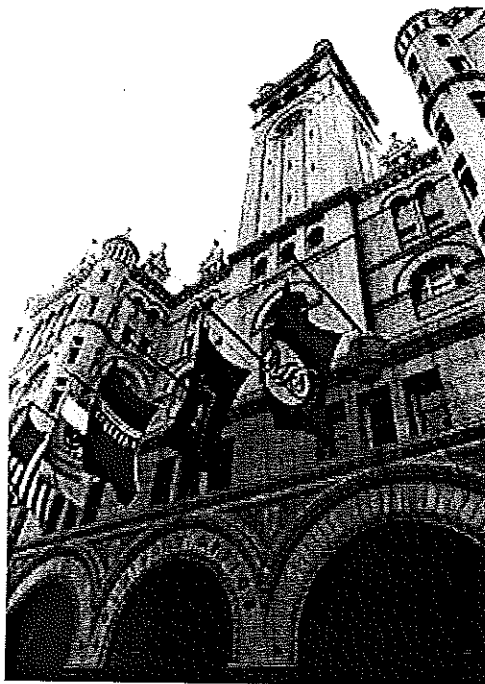


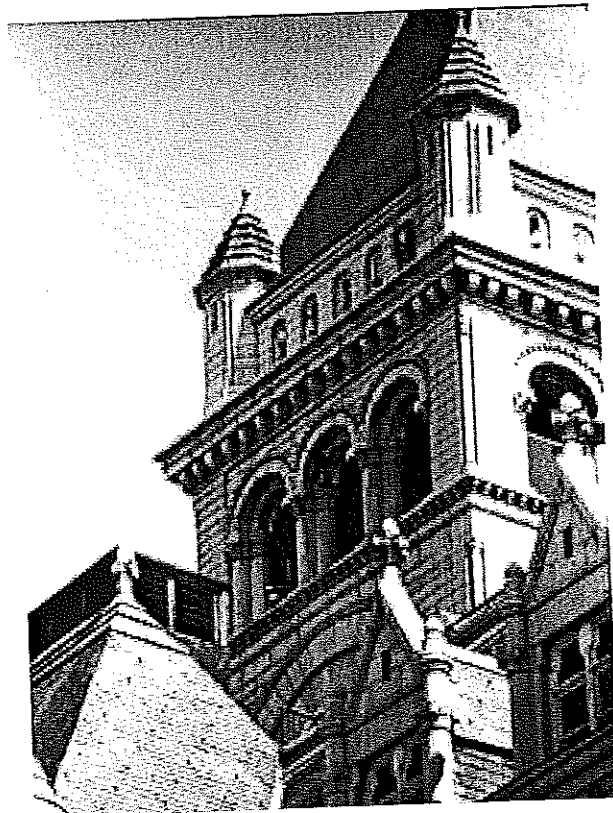
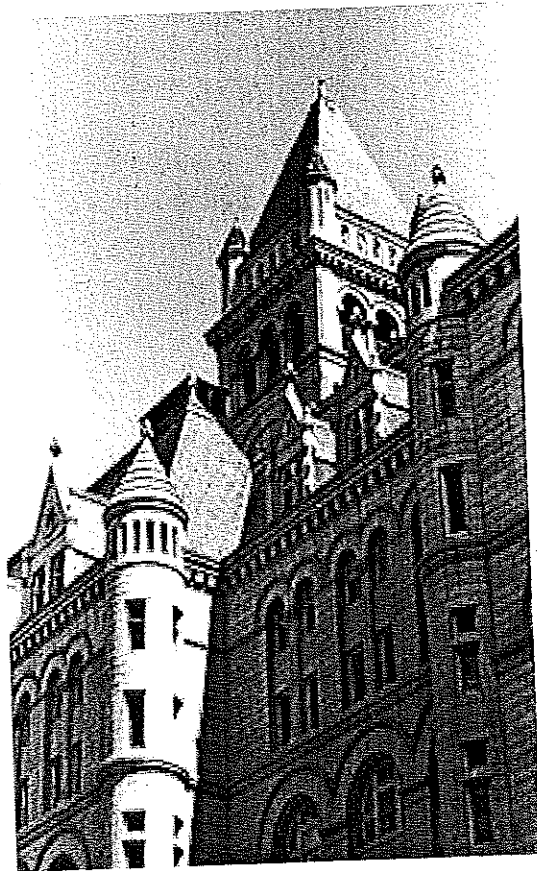


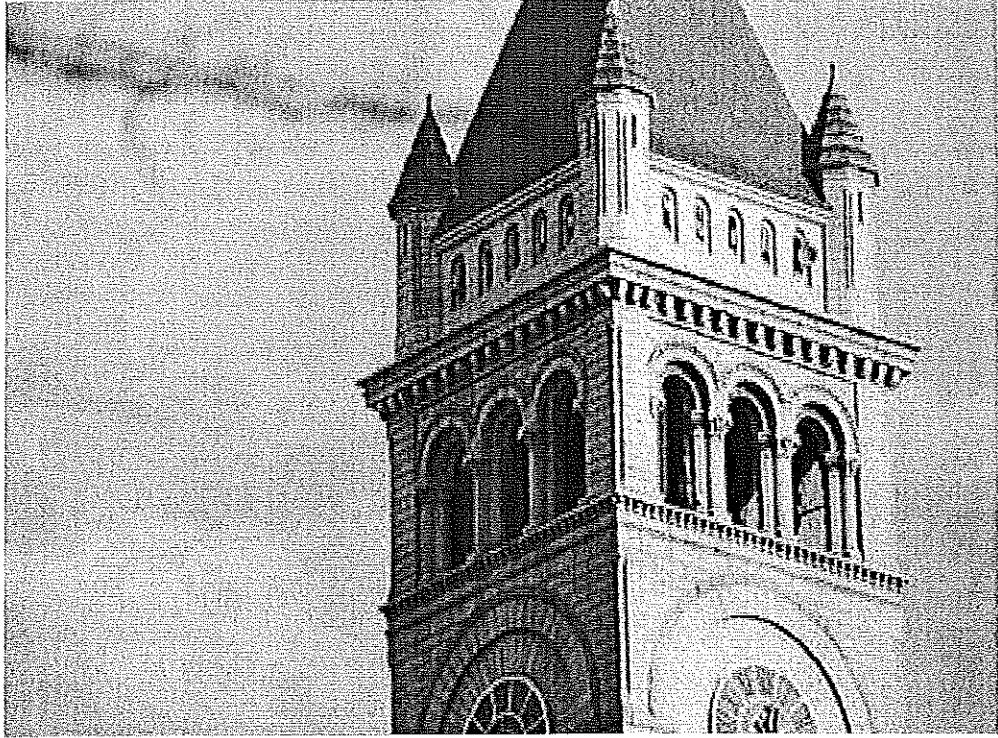


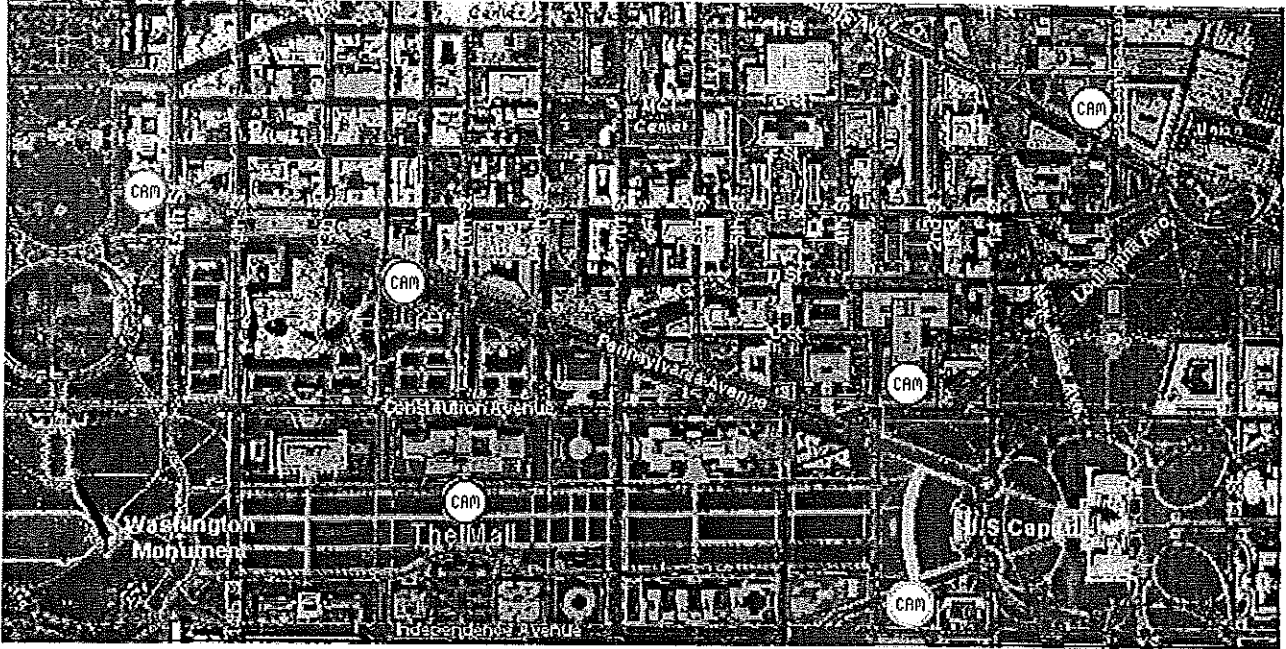



This sequence shows exactly how inconspicuous these cameras and their acoustic sensors truly are:









The different  icons and corresponding shaded areas indicate the location of DC Metropolitan Police Department surveillance cameras and their proposed areas of coverage as noted in the *Washington Post* on March 23, 2002.

The truth, according to Tom Colasti, president and CEO of Viisage Technologies, is that “the typical person is on a surveillance camera 30 times a day.”³² He’s in a good position to talk, seeing as how his company deployed the controversial facial recognition system at the 2001 Super Bowl. In England, however, this number increases to 300, as a result of the fact that there are almost 2.5 million surveillance cameras, with 150,000 in London alone.³³ This is sometimes referred to as the “fifth utility,” joining water, gas, electric, and telephones.³⁴

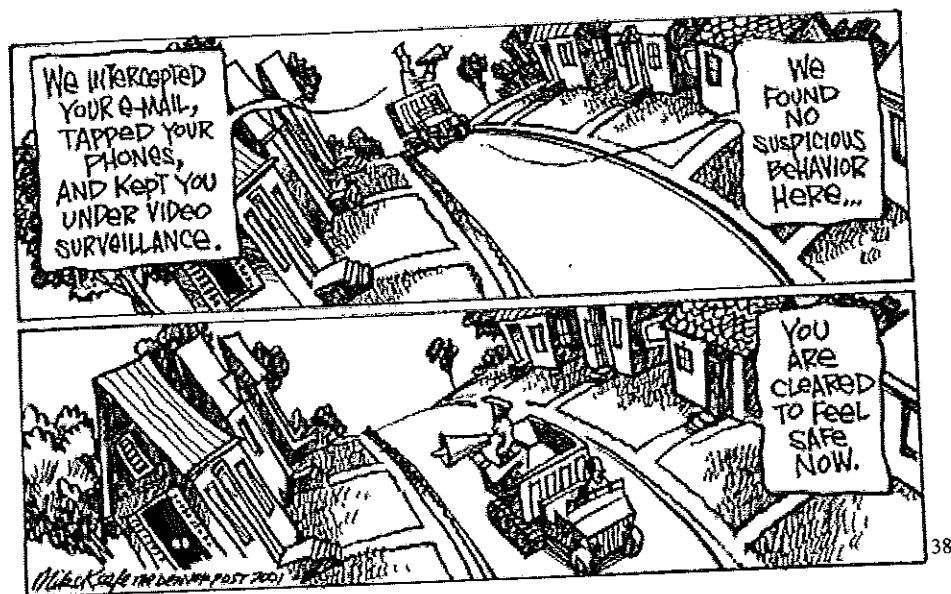
The capabilities of these systems are astounding. Cameras, thermal imaging, night vision, pattern-recognition algorithms, databases of information, and biometric tools can all be deployed simultaneously, as one entity, forming an automated surveillance network able to track just about anyone, anywhere, at any time. Managing this technology responsibly is the key. Not surprisingly, ACLU associate director Barry Steinhardt fears

that we will have a "surveillance society where none of the detail of our daily lives will escape notice and where much of that detail will be recorded."³⁵

Winston describes what this feels like in Oceana in 1984:

There was of course no way of knowing whether you were being Watched at any given moment... You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.³⁶

Johnny Barnes, Executive Director of the ACLU of the National Capital Area, suggested in a press release that British surveillance cameras have not stopped crime, which is the rationale the government is trying to sell the American people on. There are two primary reasons. First, criminals learn to stay out of camera view. Second, when criminals realize that they cannot do that, they go elsewhere, the so-called displacement effect, so that crime rates are not reduced. He indicates that surveillance cameras reduce resources for placing police officers into neighborhoods where they are needed. He also states the obvious that surveillance cameras are subject to great abuse and may intensify racial profiling.³⁷



George Washington University Professor Jeffrey Rosen provided the following account concerning surveillance camera abuse, in the *New York Times Magazine* of October 7, 2001:

Britain's experience under the watchful eye of the CCTV cameras is a vision of what American can expect if we choose to go down the same road in our efforts to achieve "homeland security." Although the cameras in Britain were initially justified as a way of combating terrorism, they soon came to serve a very different function. The cameras are designed not to produce arrests but to make people feel that they are being watched at all times. Instead of keeping terrorists off planes, biometric surveillance is being used to keep punks out of shopping malls. The people behind the live video screens are zooming in on unconventional behavior in public that in fact has nothing to do with terrorism. And rather than thwarting serious crime, the cameras are being used to enforce social conformity in ways that Americans may prefer to avoid.³⁹

New York City isn't far behind. Over the last several months, a small but dedicated group of New York Civil Liberties Union volunteers walked the streets of Manhattan, and produced a map of 2,397 *visible* cameras.⁴⁰ The word "visible" is stressed because it's quite possible that even all of these cameras could just be decoys for near invisible cameras, whose true number is unattainable, and probably always will be.

An often overlooked concern with surveillance cameras is the health hazards that they impose on the populations they monitor. The NYPD has installed clusters of microwave relay antennae in order to transmit and receive images from hand-held video cameras, which are useful for parades, demonstrations, and protests. The NYPD's relays are short and thick, and are most often installed in groups on penthouses, rooftops, and parapets. This is unfortunate, because unlike cell phone antennae which radiate their signals in all directions, microwaves beam their signals. Short term exposure to microwave radiation causes headaches, skin burns, heat exhaustion, heat stroke, and

cataracts. Long-term exposure, however, can cause sterility, leukemia, brain cancer, and lymphoma. The general public is most likely oblivious to this little fact. Ironically, these cameras endanger the public's health, all in the name of protecting its security.⁴¹

Another recent abuse is the unveiling of the total global spy network, otherwise known as Echelon. Technologically speaking, Echelon is the epitome of Big Brother, and apparently has been for quite sometime. Its activities are pursuant to the UKUSA agreement of 1947. The original Echelon dates back to 1971. Project Echelon is an automated global interception and relay system operated by intelligence agencies in five nations: the United States, UK, Canada, Australia, and New Zealand. The US National Security Agency is the lead intelligence agency. Echelon intercepts as many as 3 billion communications every day, including phone calls, email, Internet downloads, and satellite transmissions. It sifts through an estimated 90 percent of all Internet traffic. It even has special underwater devices to tap ocean cables.⁴² The system then takes all of this information and applies a dictionary of code words to help search for evidence of international crime or terrorism, or anything else the powers that be want to know. (For a brief listing of these words, see Appendix E).

The original purpose of Echelon was to protect national security during the Cold War. Now, however, it appears that industrial espionage has become part of Echelon's activities. Much of what the system intercepts it hands to top American corporations to give them an edge over their competition. Moreover, there are concerns that its actions may even be used to stifle political dissent, such as the alleged secret surveillance of Amnesty International. Apparently, even Diana, Princess of Wales, was under Echelon surveillance before her death.⁴³

Journalist Duncan Campbell, in a report commissioned by the European Parliament about Project Echelon, announced that “there are no safeguards, no remedies. There’s nowhere you can go to say that they’ve been snooping on your international communications. It’s a totally lawless world.”⁴⁴



45

It is becoming quite apparent that we live in a snitch culture, one in which citizens are now being turned into the eyes and ears of the state. As Jim Redden observes in his book *Snitch Culture*, “You can’t trust anyone these days—and it’s no accident. Children turn their parents into the police on two-bit drug charges. Classmates tattle on one another to school officials. Friends rat each other out to the authorities. Political advocacy groups report suspected dissidents to the FBI. Employers hire undercover agents to spy on workers. Lawyers are forced to report clients who pay with cash to law enforcement agencies.”⁴⁶ Indeed, as Winston warns in 1984, “The espionage, the betrayals, the arrests,

the tortures, the executions, the disappearances will never cease. It will be a world of terror as much as a world of triumph.⁴⁷

Endnotes

- 1 Darryl Cagle, home page, <http://cagle.slate.msn.com/>.
- 2 <http://www.apple.com>
- 3 George Orwell. 1984, (New York: Signet Classic, 1950), 35.
- 4 Orwell, 35.
- 5 Central Intelligence Agency. <http://www.cia.gov/ic/icagen2.htm>
- 6 Joshua Meyrowitz, No Sense of Place, (New York: Oxford University Press, 1985), 322.
- 7 Jeremy Rifkin, The Age of Access, (New York: Tarcher/Putnam, 2001), 14.
- 8 Orwell, 82.
- 9 <http://www.grocerynetwork.com>
- 10 Mitchell M Waldrop, "Grid Computing," Technology Review May 2002: 30-37.
- 11 Darryl Cagle, home page, <http://cagle.slate.msn.com/>.
- 12 Julia Scheeres, "A Satellite Baby-Sitting Service," Wired News, 2 May 2002.
- 13 Christopher Newton, "U.S. to Weigh Computer Chip Implant," Associated Press, 26 Feb. 2002.
- 14 Scheeres, 2.
- 15 *Ibid.*, 2.
- 16 *Ibid.*
- 17 Darryl Cagle, home page, <http://cagle.slate.msn.com/>.
- 18 Sherrie Gossett, "Post- 9/11 Security Fears Usher in Subdermal Chips," WorldNetDaily, 4 Feb. 2002.
- 19 Orwell, 30.
- 20 Ira Flatow, "Analysis: New Surveillance Techniques and How They May Impinge Upon Civil Liberties," National Public Radio, 5 October 2001.
- 21 Darryl Cagle, home page, <http://cagle.slate.msn.com/>.
- 22 <http://www.aclu.org/congress/L110101a.html>.
- 23 *Ibid.*
- 24 *Ibid.*
- 25 Jon Dougherty, "Is Anti-Terrorism Anti-Constitution?" WorldNetDaily, 30 Oct. 2001 .
- 26 *Ibid.*
- 27 *Ibid.*
- 28 Jon Dougherty, "Emergency-Powers Bill Gaining Momentum," WorldNetDaily, 20 March 2002.
- 29 *Ibid.*
- 30 *Ibid.*
- 31 <http://www.epic.org>.
- 32 Ira Flatow, "Analysis: New Surveillance Techniques and How They May Impinge Upon Civil Liberties," National Public Radio, 5 October 2001.
- 33 Johnny Barnes, "Privacy vs. Security: Electronic Surveillance Cameras in the District of Columbia," (ACLU, 22 Mar. 2002).
- 34 Ivan Amato, "Big Brother Logs On," Technology Review September 2001, 60.
- 35 *Ibid.*
- 36 Orwell, 6-7.
- 37 Barnes, 3.

-
- ³⁸ Darryl Cagle, home page, <http://cagle.slate.msn.com/>.
- ³⁹ Ibid., 5.
- ⁴⁰ <http://www.mediaeater.com/cameras/summary.html>.
- ⁴¹ <http://www.notbored.org/microwaves.html>.
- ⁴² "Answers to Frequently Asked Questions (FAQ) about Echelon," 7 Feb. 2001, <http://www.aclu.org/echelonwatch/faq/html>.
- ⁴³ Ibid.
- ⁴⁴ Andrew Bromford, "Echelon Spy Network Revealed," BBC 3 Nov. 1999. http://www.bbc.co.uk/hi/english/world/newsid_503000/503224.stm.
- ⁴⁵ Darryl Cagle, home page, <http://cagle.slate.msn.com/>.
- ⁴⁶ Jim Redden, Snitch Culture (Venice, CA: Feral House, 2000), 240.
- ⁴⁷ Orwell, 221.

The Hope for Humanity

Perhaps Erich Fromm poses the most poignant question of all concerning dystopian societies in his afterward to *1984*: "... can human nature be changed in such a way that man will forget his longing for freedom, for dignity, for integrity, for love—that is to say, can man forget that he is human? Or does human nature have a dynamism which will react to the violation of these basic human needs by attempting to change an inhuman society into a human one?"¹

Let's hope so, because the revelations of the previous two chapters provide a very miserable outlook for the future of America. But, the truth hurts. Most people aren't aware of the majority of what has been discussed thus far. Sadly, most would rather live by the cliché *ignorance is bliss*. The truth needs to be told.

There's an interesting psychological truth about conspiracy theories. No matter how dismal they may appear to be, conspiracies, ironically, provide a sigh of relief for human beings. No matter what the consequences may be, conspiracies mean that at least another human being, somewhere, somehow, still has control over what happens to all of us, and that our lives are not the result of random, uncontrollable, and unforeseeable events.

Not *everyone* in the government is corrupt or part of some evil plot to take over the world. A perfect example is James Pavitt, the CIA Deputy Director of Operations (DDO). In an address delivered by Pavitt at an April 11th conference at Duke University, he stated that mounting foolproof countermeasures against terrorism would require sacrificing many civil liberties which make American society great, and, as a result, would produce a system that, in his view, “is not worth defending.”² Having a CIA DDO make a statement like this is very reassuring.

Likewise, a “US Supreme Court decision last June [which] determined that in the absence of a search warrant, the government’s use of a thermal imaging device to monitor heat coming off the walls of a suspected marijuana grower’s private residence in Florence, OR, violated the Fourth Amendment prohibition against ‘unreasonable search and seizures.’”³ Of course it would be interesting to see how the court would have ruled if the case had taken place in the post 9/11 era. Nevertheless, the ruling still stands and has set a precedent that the highest court in our land now must follow.

Admittedly, positive articles are scarce. In fact, the quote from the CIA Deputy Director of Operations was lifted from an article which discussed the next unavoidable terrorist attack. Such apparent contradictions are common, as evidenced by the President telling America that all is well while his Attorney General declares that another attack is inevitable. Clear communication is essential.



THE YIN AND YANG OF IT,,,'

Computers have made it possible for loved ones in far off places to communicate with each other in ways never dreamed of a generation ago. So what if the government intercepts a message between a husband and wife, or a child and his mother, separated thousands of miles apart? Why would the government care? Logically it would seem to be a waste of time.

On a different note, so what if English becomes the universal language as a result of the Internet? It's not entirely bad. Forcing people in other countries to learn English in order to navigate the web would increase literacy, would it not? At least then there would be a universal language for all people to communicate in. And who cares if humans eventually forget how to write or type as a result of advancing technology? Illiterate people still have thoughts, wants, and needs. Technology is finally giving otherwise presumed silent people a voice. The Internet makes possible friendships between individuals and between groups of people that otherwise would never have a chance to

meet, or maybe would never want to meet. It breaks down the social barriers of traditional forms of communication.

We can't afford to ignore the warnings of Orwell's prophecy just because 1984 didn't turn out like *1984*. On the other hand, we still do have freedom of the press in this country. If we didn't, the research for this senior thesis never would have been possible.

Endnotes

¹ Erich Fromm, afterword to 1984, by George Orwell (New York: Signet Classic, 1950), 260.

² "Top CIA Official Warns Next Terror Attack Unavoidable," Yahoo!News
<http://sg.news.yahoo.com/020428/1/2onzi.html>.

³ Ivan Amato, "Big Brother Logs On," Technology Review September 2001, 63.

Bibliography

- Amato, Ivan. "Big Brother Logs On." Technology Review Sept. 2001: 60.
- "Answers to Frequently Asked Questions (FAQ) about Echelon." ACLU. Home page
7 Feb. 2001. <http://www.aclu.org/echelonwatch/faq/html>.
- Apple Computer Corporation. Home page. <http://www.apple.com>.
- Barnes, Johnny. "Privacy vs. Security: Electronic Surveillance Cameras in the District of
Columbia." Address. 22 Mar. 2002.
<http://www.dwatch.com/issues/privacy7.htm>.
- Beason, Eric. Personal interview. 27 April 2002.
- Bishop, Greg. "The Covert News Network." Disinformation: You Are Being Lied To.
Ed. Russ Kick. China: The Disinformation Company Ltd., 2002.
- Bloom, Howard. "Reality Is A Shared Hallucination." Disinformation: You Are Being
Lied To. Ed. Russ Kick. China: The Disinformation Company Ltd., 2002.
- Boorstin, Daniel J. The Discoverers: A History of Man's Search to Know His World and
Himself. New York: Vintage Books, 1985.
- Bromford, Andrew. "Echelon Spy Network Revealed." BBC 3 Nov. 1999.
http://www.bbc.co.uk/hi/english/world/newsid_503000/503224.stm.
- Cagle, Daryl. Home Page. May 2002. <http://cagle.slate.msn.com>.

Central Intelligence Agency. Home page. <http://www.cia.gov>.

Chomsky, Noam. Media Control: The Spectacular Achievements of Propaganda.

Canada: Seven Stories Press, 1997.

Chomsky, Noam. Address. "What Makes Mainstream Media Mainstream."

Z Media Institute, June 1997.

Congress. Home page. American Civil Liberties Union.

<http://www.aclu.org/congress/L110101a.html>.

Cullinan, Bernice. Children's Literature in the Reading Program. Newark, DE: IRA,

1987.

Diamond, Jared. "The Fellow Frog, Name Belong-Him Dakwo." Natural History

April 1989: 16-23.

Dougherty, Jon. "Emergency Powers Bill Gaining Momentum." WorldNetDaily

20 Mar. 2002. <http://www.worldnetdaily.com>.

Dougherty, Jon. "Is Anti-Terrorism Anti-Constitution?" WorldNetDaily

30 Oct. 2001. <http://www.worldnetdaily.com>.

Electronic Privacy Information Center. Home page. <http://www.epic.org>.

Flatow, Ira. "Analysis: New Surveillance Techniques and How They May Impinge

Upon Civil Liberties." National Public Radio 5 Oct. 2001.

Fromm, Erich. Afterword. 1984. By George Orwell. New York: Signet Classic, 1950.

Gitlin, Todd. Media Unlimited. New York: Metropolitan Books, 2001.

Goleman, Daniel. "Infants Under Two Seem To Learn From TV." New York Times

22 Nov. 1988.

Gossett, Sherrie. "Post- 9/11 Security Fears Usher in Subdermal Chips." WorldNetDaily.
4 Feb. 2002.

Healey, Jane M. Endangered Minds. New York: Touchstone, 1999.

Hotz, Lee. "The Impassioned Fight to Save Dying Languages." LA Times Online, 2000.

Kick, Russ. Disinformation: You Are Being Lied To. China: The Disinformation
Company, 2002.

Korpela, Jukka. "English, the Universal Language on the Internet?" Home page.
<http://www.cs.tut.fi/~jkorpela/lingua-franca.html>.

Lakoff, George. Metaphors We Live By Chicago: University of Chicago Press, 1981.

Lester, Will. "Reinvention of Language Thrives." Associated Press 2 Feb. 2001.

Loftus, Elizabeth. Memory: Surprising New Insights Into How We Remember and Why
We Forget. Reading, MA: Addison Wesley, 1980.

MediaEater. Home page. <http://www.mediaeater.com/cameras/summary.html>.

Meyrowitz, Joshua. No Sense of Place. New York: Oxford University Press, 1985.

Newton, Christopher. "U.S. To Weigh Computer Chip Implant." Associated Press
26 Feb. 2002.

Notbored. Home page. <http://www.notbored.org/microwaves.html>.

Orwell, George. 1984. New York: Signet Classic, 1950.

Orwell, George. "Politics and the English Language." Essay. 1946.

Postman, Neil. Amusing Ourselves to Death. New York: Penguin Books Ltd., 1985.

Redden, Jim. Snitch Culture. Venice, CA: Feral House, 2000.

Rifkin, Jeremy. The Age of Access. New York: Oxford University Press, 1985.

Scheeres, Julia. "A Satellite Baby-Sitting Service." Wired News 2 May 2002.

- Shanahan, Angela. "Language in Moral Straights." The Australian. 27 Nov. 2001.
- Slobin, Dan. "Language and Thought." Essay. U of California at Berkely, 1996.
- Stearns, Peter N. "The Rise of Sibling Jealousy in the Twentieth Century." Emotion and Social Change: Toward a New Psychohistory. New York: Holmes and Meier, 1988: 197-209.
- "The Simpsons—New Kids on the Bleccch." 25 Feb. 2001. Home page. Kidzworld. <http://www.kidzworld.com/site/p461.htm>.
- "Top CIA Official Warns Next Terror Attack Unavoidable." Yahoo!News. <http://sg.news.yahoo.com/020428/1/2onzj.html>.
- Vail, Priscilla. Smart Kids With School Problems. New York: NAL, 1989.
- Waldrop, Mitchell M. "Grid Computing." Technology Review. May 2002: 30-37.
- Wurman, Richard Saul. Information Anxiety. New York: Double Day, 1989.
- Zigler, E. and Frank M. The Parental Leave Crisis. New Haven: Yale University Press, 1988.

Appendices

Appendix A: United States Bill of Rights

Appendix B: USA Patriot Act

Appendix C: H.R. 2459 Establishment of Department of Peace

Appendix D: Fact Sheet on Office of Homeland Security

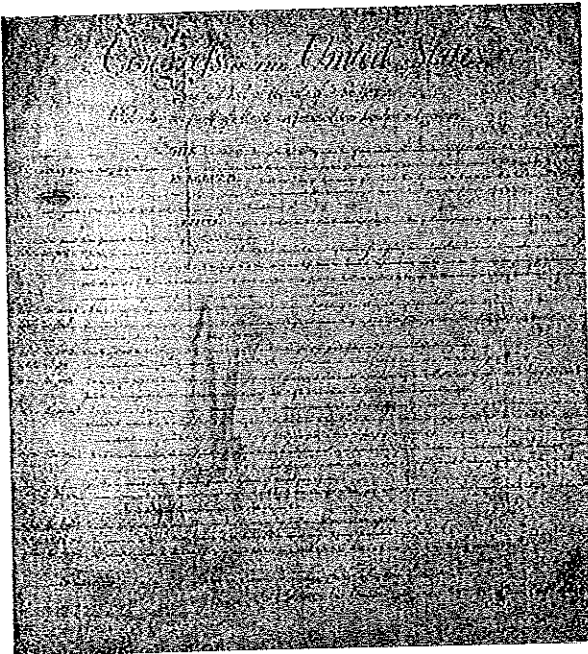
Appendix E: Echelon Code Words

Appendix A: United States Bill of Rights



The Bill of Rights

During the debates on the adoption of the Constitution, its opponents repeatedly charged that the Constitution as drafted would open the way to tyranny by the central government. Fresh in their minds was the memory of the British violation of civil rights before and during the Revolution. They demanded a "bill of rights" that would spell out the immunities of individual citizens. Several state conventions in their formal ratification of the Constitution asked for such amendments; others ratified the Constitution with the understanding that the amendments would be offered.



On September 25, 1789, the First Congress of the United States therefore proposed to the state legislatures 12 amendments to the Constitution that met arguments most frequently advanced against it. The first two proposed amendments, which concerned the number of constituents for each Representative and the compensation of Congressmen, were not ratified. Articles 3 to 12, however, ratified by three-fourths of the state legislatures, constitute the first 10 amendments of the Constitution, known as the Bill of Rights.

You can read a transcription of [the preamble](#), [amendments 1-10](#), and [amendments 11-27](#) of the Constitution.

Note: The above image is the joint resolution of Congress proposing 12 articles as amendments to the Constitution and was enrolled on parchment by William Lambert, a Clerk of the House. It was signed by Frederick Augustus Muhlenberg, Speaker of the House, on September 28, 1789, and by John Adams, President of the Senate, shortly thereafter. The Bill of Rights, as this parchment copy is now known, is on permanent display in the Rotunda of the National Archives. You can display a [high-resolution image](#) of the Bill of Rights (339K JPEG).

A Voice of Dissent: George Mason



[Bill of Rights page](#)

THE PREAMBLE TO THE BILL OF RIGHTS

Congress of the United States
begun and held at the City of New-York, on
Wednesday the fourth of March, one thousand seven hundred and eighty nine.

THE Conventions of a number of the States, having at the time of their adopting the Constitution, expressed a desire, in order to prevent misconstruction or abuse of its powers, that further declaratory and restrictive clauses should be added: And as extending the ground of public confidence in the Government, will best ensure the beneficent ends of its institution.

RESOLVED by the Senate and House of Representatives of the United States of America, in Congress assembled, two thirds of both Houses concurring, that the following Articles be proposed to the Legislatures of the several States, as amendments to the Constitution of the United States, all, or any of which Articles, when ratified by three fourths of the said Legislatures, to be valid to all intents and purposes, as part of the said Constitution; viz.

ARTICLES in addition to, and Amendment of the Constitution of the United States of America, proposed by Congress, and ratified by the Legislatures of the several States, pursuant to the fifth Article of the original Constitution.

[\[Amendments 1-10\]](#) [\[Amendments 11-27\]](#)

Note: The capitalization and punctuation in this version are from the enrolled original of the Joint Resolution of Congress proposing the [Bill of Rights](#), which is on permanent display in the Rotunda of the National Archives Building, Washington, D.C.

National Archives and Records Administration home page
URL: <http://www.nara.gov/exhall/charters/billrights/preamble.html>
inquire@nara.gov
Last Modified on April 25, 2001



As the delegates gathered at the Pennsylvania State House in May 1787 to "revise" the Articles of Confederation, Virginia delegate George Mason wrote, "The Eyes of the United States are turned upon this Assembly and their Expectations raised to a very anxious Degree." Mason had earlier written the Virginia Declaration of Rights that strongly influenced Thomas Jefferson in writing the first part of the Declaration of Independence. He left the convention bitterly disappointed, however, and became one of the Constitution's most vocal opponents. "It has no declaration of rights," he was to state. Ultimately, George Mason's views prevailed. When James Madison drafted the amendments to the Constitution that were to become the Bill of Rights, he drew heavily upon the ideas put forth in the Virginia Declaration of Rights.

The article "A More Perfect Union" provides an in-depth look at the Constitutional Convention, the ratification process, and the adoption of the Bill of Rights.

[[Constitution](#) | [Declaration of Independence](#) | [Charters Page](#) | [Exhibit Hall](#)]



[National Archives and Records Administration](#)

URL: <http://www.nara.gov/exhall/charters/billrights/billmain.html>

inquire@nara.gov

Last updated: January 29, 1998



THE FIRST 10 AMENDMENTS TO THE CONSTITUTION AS RATIFIED BY THE STATES

Note: The following text is a transcription of the first 10 amendments to the Constitution in their original form. These amendments were ratified December 15, 1791, and form what is known as the "Bill of Rights."

Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

Amendment II

A well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not be infringed.

Amendment III

No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.

Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Amendment V

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Amendment VI

In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defence.

Amendment VII

In suits at common law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved, and no fact tried by a jury, shall be otherwise reexamined in any Court of the United States, than according to the rules of the common law.

Amendment VIII

Excessive bail shall not be required, nor excessive fines imposed, nor cruel and unusual punishments inflicted.

Amendment IX

The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

Amendment X

The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.

Amendments 11-27

Note: The capitalization and punctuation in this version is from the enrolled original of the Joint Resolution of Congress proposing the Bill of Rights, which is on permanent display in the Rotunda of the National Archives Building, Washington, D.C.

National Archives and Records Administration home page
URL: <http://www.nara.gov/exhall/charters/billrights/billrights.html>
inquire@nara.gov
Last Modified on December 10, 2001

Amendments 11-27 to the Constitution of the United States

[[Constitution](#) | [Bill of Rights](#) | [Charters Page](#) | [Exhibit Hall](#)]

AMENDMENT XI

Passed by Congress March 4, 1794. Ratified February 7, 1795.

Note: Article III, section 2, of the Constitution was modified by amendment 11.

The Judicial power of the United States shall not be construed to extend to any suit in law or equity, commenced or prosecuted against one of the United States by Citizens of another State, or by Citizens or Subjects of any Foreign State.

AMENDMENT XII

Passed by Congress December 9, 1803. Ratified June 15, 1804.

Note: A portion of Article II, section 1 of the Constitution was superseded by the 12th amendment.

The Electors shall meet in their respective states and vote by ballot for President and Vice-President, one of whom, at least, shall not be an inhabitant of the same state with themselves; they shall name in their ballots the person voted for as President, and in distinct ballots the person voted for as Vice-President, and they shall make distinct lists of all persons voted for as President, and of all persons voted for as Vice-President, and of the number of votes for each, which lists they shall sign and certify, and transmit sealed to the seat of the government of the United States, directed to the President of the Senate; -- the President of the Senate shall, in the presence of the Senate and House of Representatives, open all the certificates and the votes shall then be counted; -- The person having the greatest number of votes for President, shall be the President, if such number be a majority of the whole number of Electors appointed; and if no person have such majority, then from the persons having the highest numbers not exceeding three on the list of those voted for as President, the House of Representatives shall choose immediately, by ballot, the President. But in choosing the President, the votes shall be taken by states, the representation from each state having one vote; a quorum for this purpose shall consist of a member or members from two-thirds of the states, and a majority of all the states shall be necessary to a choice. [And if the House of Representatives shall not choose a President whenever the right of choice shall devolve upon them, before the fourth day of March next following, then the Vice-President shall act as President, as in case of the death or other constitutional disability of the President. --]* The person having the greatest number of votes as Vice-President, shall be the Vice-President, if such number be a majority of the whole number of Electors appointed, and if no person have a majority, then from the two highest numbers on the list,

Section 3.

No person shall be a Senator or Representative in Congress, or elector of President and Vice-President, or hold any office, civil or military, under the United States, or under any State, who, having previously taken an oath, as a member of Congress, or as an officer of the United States, or as a member of any State legislature, or as an executive or judicial officer of any State, to support the Constitution of the United States, shall have engaged in insurrection or rebellion against the same, or given aid or comfort to the enemies thereof. But Congress may by a vote of two-thirds of each House, remove such disability.

Section 4.

The validity of the public debt of the United States, authorized by law, including debts incurred for payment of pensions and bounties for services in suppressing insurrection or rebellion, shall not be questioned. But neither the United States nor any State shall assume or pay any debt or obligation incurred in aid of insurrection or rebellion against the United States, or any claim for the loss or emancipation of any slave; but all such debts, obligations and claims shall be held illegal and void.

Section 5.

The Congress shall have the power to enforce, by appropriate legislation, the provisions of this article.

**Changed by section 1 of the 26th amendment.*

AMENDMENT XV

Passed by Congress February 26, 1869. Ratified February 3, 1870.

Section 1.

The right of citizens of the United States to vote shall not be denied or abridged by the United States or by any State on account of race, color, or previous condition of servitude--

Section 2.

The Congress shall have the power to enforce this article by appropriate legislation.

AMENDMENT XVI

Passed by Congress July 2, 1909. Ratified February 3, 1913.

Note: Article I, section 9, of the Constitution was modified by amendment 16.

The Congress shall have power to lay and collect taxes on incomes, from whatever source derived, without apportionment among the several States, and without regard to any census or enumeration.

AMENDMENT XVII

AMENDMENT XX

Passed by Congress March 2, 1932. Ratified January 23, 1933.

Note: Article I, section 4, of the Constitution was modified by section 2 of this amendment. In addition, a portion of the 12th amendment was superseded by section 3.

Section 1.

The terms of the President and the Vice President shall end at noon on the 20th day of January, and the terms of Senators and Representatives at noon on the 3d day of January, of the years in which such terms would have ended if this article had not been ratified; and the terms of their successors shall then begin.

Section 2.

The Congress shall assemble at least once in every year, and such meeting shall begin at noon on the 3d day of January, unless they shall by law appoint a different day.

Section 3.

If, at the time fixed for the beginning of the term of the President, the President elect shall have died, the Vice President elect shall become President. If a President shall not have been chosen before the time fixed for the beginning of his term, or if the President elect shall have failed to qualify, then the Vice President elect shall act as President until a President shall have qualified; and the Congress may by law provide for the case wherein neither a President elect nor a Vice President shall have qualified, declaring who shall then act as President, or the manner in which one who is to act shall be selected, and such person shall act accordingly until a President or Vice President shall have qualified.

Section 4.

The Congress may by law provide for the case of the death of any of the persons from whom the House of Representatives may choose a President whenever the right of choice shall have devolved upon them, and for the case of the death of any of the persons from whom the Senate may choose a Vice President whenever the right of choice shall have devolved upon them.

Section 5.

Sections 1 and 2 shall take effect on the 15th day of October following the ratification of this article.

Section 6.

This article shall be inoperative unless it shall have been ratified as an amendment to the Constitution by the legislatures of three-fourths of the several States within seven years from the date of its submission.

AMENDMENT XXI

Passed by Congress February 20, 1933. Ratified December 5, 1933.

Section 1.

The eighteenth article of amendment to the Constitution of the United States is hereby repealed.

AMENDMENT XXIV

Passed by Congress August 27, 1962. Ratified January 23, 1964.

Section 1.

The right of citizens of the United States to vote in any primary or other election for President or Vice President, for electors for President or Vice President, or for Senator or Representative in Congress, shall not be denied or abridged by the United States or any State by reason of failure to pay poll tax or other tax.

Section 2.

The Congress shall have power to enforce this article by appropriate legislation.

AMENDMENT XXV

Passed by Congress July 6, 1965. Ratified February 10, 1967.

Note: Article II, section 1, of the Constitution was affected by the 25th amendment.

Section 1.

In case of the removal of the President from office or of his death or resignation, the Vice President shall become President.

Section 2.

Whenever there is a vacancy in the office of the Vice President, the President shall nominate a Vice President who shall take office upon confirmation by a majority vote of both Houses of Congress.

Section 3.

Whenever the President transmits to the President pro tempore of the Senate and the Speaker of the House of Representatives his written declaration that he is unable to discharge the powers and duties of his office, and until he transmits to them a written declaration to the contrary, such powers and duties shall be discharged by the Vice President as Acting President.

Section 4.

Whenever the Vice President and a majority of either the principal officers of the executive departments or of such other body as Congress may by law provide, transmit to the President pro tempore of the Senate and the Speaker of the House of Representatives their written declaration that the President is unable to discharge the powers and duties of his office, the Vice President shall immediately assume the powers and duties of the office as Acting President.

Thereafter, when the President transmits to the President pro tempore of the Senate and the Speaker of the House of Representatives his written declaration that no inability exists, he shall resume the powers and duties of his office unless the Vice President and a majority of either the principal officers of the executive department or of such other body as Congress may by law provide, transmit within four days to the President pro tempore of the Senate and the Speaker of the House of Representatives their written declaration that the President is unable to discharge the powers and duties of his office. Thereupon Congress shall decide

Appendix B: USA Patriot Act Appendices

VI. APPENDICES

Appendix A: Sample Network Banner Language

Network banners are electronic messages that provide notice of legal rights to users of computer networks. From a legal standpoint, banners have four primary functions. First, banners may be used to generate consent to real-time monitoring under Title III. Second, banners may be used to generate consent to the retrieval of stored files and records pursuant to ECPA. Third, in the case of government networks, banners may eliminate any Fourth Amendment “reasonable expectation of privacy” that government employees or other users might otherwise retain in their use of the government’s network under O’Connor v. Ortega, 480 U.S. 709 (1987). Fourth, in the case of a non-government network, banners may establish a system administrator’s “common authority” to consent to a law enforcement search pursuant to United States v. Matlock, 415 U.S. 164 (1974).

CCIPS does not take any position on whether providers of network services should use network banners, and, if so, what types of banners they should use. Further, there is no formal “magic language” that is necessary. However, it is important to realize that banners may be worded narrowly or broadly, and the scope of consent and waiver triggered by a particular banner will in general depend on the scope of its language. Here is a checklist of issues that may be considered when drafting a banner:

- a) Does the banner state that use of the network constitutes consent to monitoring? Such a statement helps establish the user’s consent to real-time interception pursuant to 18 U.S.C. § 2511(2)(d).
- b) Does the banner state that use of the network constitutes consent to the retrieval and disclosure of information stored on the network? Such a statement helps establish the user’s consent to the retrieval and disclosure of stored information pursuant to 18 U.S.C. § 2702(b)(3) and § 2703(c)(1)(B)(iii).
- c) In the case of a government network, does the banner state that a user of the network shall have no reasonable expectation of privacy in the network? Such a statement helps establish that the user lacks a reasonable expectation of privacy pursuant to O’Connor v. Ortega, 480 U.S. 709 (1987).
- d) In the case of a non-government network, does the banner make clear that the network system administrator(s) may consent to a law enforcement search? Such a statement helps establish the system administrator’s common authority to consent to a search under United States v. Matlock, 415 U.S. 164 (1974).

e) Does the banner contain express or implied limitations or authorizations relating to the purpose of any monitoring, who may conduct the monitoring, and what will be done with the fruits of any monitoring?

f) Does the banner require users to “click through” or otherwise acknowledge the banner before using the network? Such a step may make it easier to establish that the network user actually received the notice that the banner is designed to provide.

Network providers who decide to banner all or part of their network should consider their needs and the needs of their users carefully before selecting particular language. For example, a sensitive government computer network may require a broadly worded banner that permits access to all types of electronic information. Here are three examples of broad banners:

- (1) *WARNING! This computer system is the property of the United States Department of Justice. The Department may monitor any activity on the system and retrieve any information stored within the system. By accessing and using this computer, you are consenting to such monitoring and information retrieval for law enforcement and other purposes. Users should have no expectation of privacy as to any communication on or information stored within the system, including information stored locally on the hard drive or other media in use with this unit (e.g., floppy disks, tapes, CD-ROMs, etc.).*
- (2) *This is a Department of Defense (DoD) computer system. DoD computer systems are provided for the processing of Official U.S. Government information only. All data contained within DoD computer systems is owned by the Department of Defense, and may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may disclose any potential evidence of crime found on DoD computer systems for any reason. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, or CAPTURING and DISCLOSURE.*
- (3) *You are about to access a United States government computer network that is intended for authorized users only. You should have no expectation of privacy in your use of this network. Use of this network constitutes consent to monitoring, retrieval, and disclosure of any information stored within the network for any purpose including criminal prosecution.*

In other cases, network providers may wish to establish a more limited monitoring policy. Here are three examples of relatively narrow banners that will generate consent to monitoring in some situations but not others:

- (4) *This computer network belongs to the Grommie Corporation and may be used only by Grommie Corporation employees and only for work-related purposes. The Grommie Corporation reserves the right to monitor use of this network to ensure network security and to respond to specific allegations of employee misuse. Use of this network shall constitute consent to monitoring for such purposes. In addition, the Grommie Corporation reserves the right to consent to a valid law enforcement request to search the network for evidence of a crime stored within the network.*
- (5) *Warning: Patrons of the Cyber-Fun Internet Café may not use its computers to access, view, or obtain obscene materials. To ensure compliance with this policy, the Cyber-Fun Internet Café reserves the right to record the names and addresses of World Wide Web sites that patrons visit using Cyber-Fun Internet Café computers.*
- (6) *It is the policy of the law firm of Rowley & Yzaguirre to monitor the Internet access of its employees to ensure compliance with law firm policies. Accordingly, your use of the Internet may be monitored. The firm reserves the right to disclose the fruits of any monitoring to law enforcement if it deems such disclosure to be appropriate.*

Appendix B: Sample 18 U.S.C. § 2703(d)
Application and Order

UNITED STATES DISTRICT COURT
FOR THE _____ DISTRICT OF _____

)	
IN RE APPLICATION OF THE)	
UNITED STATES OF AMERICA FOR)	MISC. NO. _____
AN ORDER PURSUANT TO)	
18 U.S.C. § 2703(d))	Filed Under Seal

APPLICATION

[Name], an Assistant United States Attorney for the _____ District of _____, hereby files under seal this ex parte application for an order pursuant to 18 U.S.C. Section 2703(d) to require [Internet Service Provider], [mailing address], to provide records and other information pertaining to the [Internet Service Provider] network account that was assigned Internet Protocol address [xxx.xxx.xxx.xxx] on [date] and [time].

The records and other information requested are set forth as Attachment 1 to the Application and to the proposed Order. In support of this Application, the United States offers the following:

FACTUAL BACKGROUND

1. The United States Government, including the Federal Bureau of Investigation and the Department of Justice, is investigating intrusions into a number of computers in the United States and abroad that occurred on [date], and which may be continuing. These computer intrusions are being investigated as possible violations of 18 U.S.C. § 1030 (damage and unauthorized access to a protected computer) and § 2511 (unlawful interception of electronic communications). Investigation to date of these incidents provides reasonable grounds to believe that [Internet Service Provider] has records and other information pertaining to certain of its subscribers that are relevant and material to

an ongoing criminal investigation.

2. In particular, on [date], [victim] discovered an unauthorized intrusion into its computer system, and, specifically, into the following computers: _____.

Investigation into this incident revealed that the intruder had obtained so-called “root” or system administrator level access into the _____ computer, effectively giving the intruder complete control of the system. The _____ computer is a “protected computer” according to 18 U.S.C. § 1030(e)(2). Accordingly, this unauthorized intrusion constitutes a criminal violation of 18 U.S.C. § 1030(a)(2).

3. On [date], the intruder(s) again connected to the _____ computer, and again obtained unauthorized “root” access. During that intrusion, investigators recorded the unique Internet Protocol address of the source of the intrusion, [xxx.xxx.xxx.xxx]. Investigators later determined that this address belongs to [Internet Service Provider]. [Internet Service Provider] provides both electronic communications services (access to e-mail and the Internet) and remote computing services (access to computers for the storage and processing of data) to its customers and subscribers using a range of assigned Internet Protocol addresses that include the address of the intrusion.

4. Obtaining the records of customer and subscriber information relating to the [Internet Service Provider] account that was assigned address [xxx.xxx.xxx.xxx] on [date] and [time], as well as the contents of electronic communications (not in electronic storage) associated with that account, will help government investigators identify the individual(s) who are responsible for the unauthorized access of the computer systems described above and to determine the nature and scope of the intruder’s activities. In particular, the [Internet Service Provider] customer who was assigned this Internet Protocol address at that particular time may be the person responsible for the unauthorized intrusion. Alternatively, records of the customer’s account may offer clues that will permit investigators to “trace back” the intrusion to its source.

LEGAL BACKGROUND

5. 18 U.S.C. § 2703 sets out particular requirements that the government must meet in order to obtain access to the records and other information in the possession of providers of “electronic communications services” and/or “remote computing services.” [Internet Service Provider] functions both as an electronic communications service provider ~ that is, it provides its subscribers access to electronic communication services, including e-mail and the Internet ~ and as a remote computing service provider ~ it provides computer facilities for the storage and processing of electronic communications ~ as those terms are used in 18 U.S.C. § 2703. [Note that because a “remote computing service” is public by definition, this statement must be modified if you are seeking information from a service provider who is not a provider to the public, such as, for example, a university.]

6. Here, the government seeks to obtain three categories of records: (1) basic subscriber information; (2) records and other information, including connection logs, pertaining to certain subscribers; and [Add only if the application seeks to obtain the contents of communications (such as e-mails) pursuant to § 2703(b), as opposed to mere records pursuant to § 2703(c).] (3) the content of electronic communications in a remote

computing service (but not communications in electronic storage¹).

7. To obtain basic subscriber information, such as the subscriber's name, address, billing information, and other identifying records, the government needs only a subpoena; however, the government may also compel such information through an order issued pursuant to section 2703(d). See 18 U.S.C. § 2703(c)(1)(C). To obtain other types of records and information pertaining to the subscribers or customers of service providers, including connection logs and other audit information, the government must comply with the dictates of sections 2703(c)(1)(B) and 2703(d). Section § 2703(c)(1)(B) provides in pertinent part:

A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity only when the governmental

¹“Electronic Storage” is a term of art, specifically defined in 18 U.S.C. § 2510(17) as “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” The government does not seek access to any such materials. Communications not in “electronic storage” include any e-mail communications received by the specified accounts that the owner or user of the account has already accessed, viewed, or downloaded.

entity . . . obtains a court order for such disclosure under subsection (d) of this section;

8. [Add only if the application seeks to obtain the contents of communications (such as e-mails) pursuant to § 2703(b), as opposed to mere records pursuant to § 2703(c).] To obtain the contents of electronic communications held by a remote computing service (but not the contents in “electronic storage,” *see n.1*), the government must comply with 2703(b)(1)(B), which provides, in pertinent part:

A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph 2 of this subsection . . . with prior notice from the government entity to the subscriber or customer if the governmental entity . . . obtains a court order for such disclosure under subsection (d) of this section . . . except that delayed notice may be given pursuant to section 2705 of this title.

Paragraph 2 of subsection 2703(b) applies with respect to any electronic communication that is held or maintained on a remote computing service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

Therefore, communications described by paragraph 2 of subsection 2703(b) include the content of electronic mail that has been opened, viewed, downloaded, or otherwise accessed by the recipient and is held remotely by the service provider on its computers.

9. All of the information the government seeks from [Internet Service Provider] through this application may be compelled through an order that complies with section 2703(d). Section 2703(d) provides in pertinent part:

A court order for disclosure under subsection . . . (c) may be issued by any court that is a court of competent jurisdiction described in section 3127(2)(A)² and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought, are relevant and material to an ongoing criminal investigation. . . . A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

Accordingly, this application sets forth facts showing there are reasonable grounds to believe that the materials sought are relevant and material to the ongoing criminal investigation.

GOVERNMENT'S REQUEST

10. The government requests that [Internet Service Provider] be directed to produce all records described in Attachment 1 to this Application. This information is directly relevant to identifying the individual(s) responsible for the crime under

² 18 U.S.C. § 3127(2)(A) defines the term “court of competent jurisdiction” as including “a district court of the United States (including a magistrate of such a court) or a United States Court of Appeals.” Because 18 U.S.C. § 2703(d) expressly permits “any” such court to issue an order, this Court may enter an order directing the disclosure of such information even if the information is stored outside of this judicial District.

investigation. The information requested should be readily accessible to [Internet Service Provider] by computer search, and its production should not prove to be unduly burdensome. [Undersigned should check with the ISP before filing this document to ensure the accuracy of this statement.]

11. The United States requests that this Application and Order be sealed by the Court until such time as the court directs otherwise.

12. The United States further requests that pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), that [Internet Service Provider] be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this order for such period as the court deems appropriate. The United States submits that such an order is justified because notification of the existence of this order could seriously jeopardize the ongoing investigation. Such a disclosure could give the subscriber an opportunity to destroy evidence, notify confederates, or flee or continue his flight from prosecution.

13. [Add only if the application seeks to obtain the contents of communications pursuant to § 2703(b), as opposed to mere records pursuant to § 2703(c):] The United States further requests, pursuant to the delayed notice provisions of 18 U.S.C. § 2705(a), an order delaying any notification to the subscriber or customer that may be required by § 2703(b) to obtain the contents of communications, for a period of 90 days. Providing prior notice to the subscriber or customer could seriously jeopardize the ongoing investigation, as such a disclosure would give the subscriber an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee or continue his flight from prosecution. [Optional Baker Act language to use if the ISP is a university: The United States further requests that [Internet Service Provider]’s compliance with the delayed notification provisions of this Order shall be deemed authorized under 20 U.S.C. § 1232g(b)(1)(j)(ii) (the “Baker Act”). See 34 CFR § 99.31 (a)(9)(i) (exempting requirement of prior notice for disclosures made to comply with a judicial order or lawfully issued subpoena where the disclosure is made pursuant to “any other subpoena

issued for a law enforcement purpose and the court or other issuing agency has ordered that the existence or the contents of the subpoena or the information furnished in response to the subpoena not be disclosed”).

WHEREFORE, it is respectfully requested that the Court grant the attached Order, (1) directing [Internet Service Provider] to provide the United States with the records and information described in Attachment 1; (2) directing that the Application and Order be sealed; (3) directing [Internet Service Provider] not to disclose the existence or content of the Order, except to the extent necessary to carry out the Orders; and [Use only if the application seeks to obtain the contents of communications pursuant to § 2703(b)] (4) directing that the notification by the government otherwise required by 18 U.S.C. § 2703(b) be delayed for ninety days.

Respectfully Submitted,

Assistant United States Attorney

ATTACHMENT 1

You are to provide the following information as printouts and as ASCII data files (on 8 mm helical scan tape for Unix host), if available:

A. All customer or subscriber account information for any accounts registered to _____, or associated with _____. For each such account, the information shall include:

1. The subscriber's account and login name(s);
2. The subscriber's address;
3. The subscriber's telephone number or numbers;

4. The subscriber's e-mail address;
5. Any other information pertaining to the identity of the subscriber, including, but not limited to billing information (including type and number of credit cards, student identification number, or other identifying information).

B. User connection logs for:

- (1) all accounts identified in Part A, above,
- (2) the IP address [xxx.xxx.xxx.xxx],

for the time period beginning _____ through and including the date of this order, for any connections to or from ____.

User connection logs should contain the following:

1. Connection time and date;
2. Disconnect time and date;
3. Method of connection to system (e.g., SLIP, PPP, Shell);
4. Data transfer volume (e.g., bytes);
5. Connection information for other systems to which user connected via ,

including:

- a. Connection destination;
- b. Connection time and date;
- c. Disconnect time and date;
- d. Method of connection to system (e.g., telnet, ftp, http);
- e. Data transfer volume (e.g., bytes);

C. [Add only if the application seeks to obtain the contents of communications (such as e-mails) pursuant to § 2703(b), as opposed to mere records pursuant to § 2703(c).]

The contents of electronic communications (not in electronic storage¹) that were placed or

¹ "Electronic Storage" is a term of art, specifically defined in 18 U.S.C. § 2510(17) as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication." The government does not seek access to any such materials. Communications not in "electronic

stored in directories or files owned or controlled by the accounts identified in Part A at any time after [date] up through and including the date of this Order.

storage” include any e-mail communications received by the specified accounts that the owner or user of the account has already accessed, viewed, or downloaded.

UNITED STATES DISTRICT COURT
FOR THE _____ DISTRICT OF _____

)	
IN RE APPLICATION OF THE)	
UNITED STATES OF AMERICA FOR)	MISC. NO. _____
AN ORDER PURSUANT TO)	
18 U.S.C. § 2703(d))	Filed Under Seal

ORDER

This matter having come before the court pursuant to an application under Title 18, United States Code, Section 2703(b) and (c), which application requests the issuance of an order under Title 18, United States Code, Section 2703(d) directing [Internet Service Provider], an electronic communications service provider and a remote computing service, located at [mailing address], to disclose certain records and other information, as set forth in Attachment 1 to the Application, the court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

IT APPEARING that the information sought is relevant and material to an ongoing criminal investigation, and that prior notice of this Order to any person of this investigation or this application and order by the government or [Internet Service Provider] would seriously jeopardize the investigation;

IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(d) that [Internet Service Provider] will, within [three] days of the date of this Order, turn over to agents of the Federal Bureau of Investigation the records and other information as set forth in Attachment 1 to this Order.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court, and that [Internet Service Provider] shall not disclose the existence of the Application or this Order of the Court, or the existence of the

investigation, to the listed subscriber or to any other person unless and until authorized to do so by the Court.

[Add only if the application seeks to obtain the contents of communications (such as e-mails) pursuant to § 2703(b), as opposed to mere records pursuant to § 2703(c).] IT IS FURTHER ORDERED that the notification by the government otherwise required under 18 U.S.C. § 2703(b)(1)(B) be delayed for ninety days. [Optional Baker Act language if the ISP is a university: Furthermore, [Internet Service Provider]’s compliance with the non-disclosure provision of this Order shall be deemed authorized under 20 U.S.C. § 1232g(b)(1)(j)(ii).]

United States Magistrate Judge

Date

**Appendix C: Sample Language for Preservation
Request Letters under 18 U.S.C. § 2703(f)**

[Internet Service Provider]
[Address]

VIA FAX to (xxx) xxx-xxxx

Dear Mr. []:

I am writing to confirm our telephone conversation earlier today and to make a formal request for the preservation of records and other evidence pursuant to 18 U.S.C. § 2703(f) pending further legal process.

You are hereby requested to preserve, for a period of 90 days, the records described below currently in your possession, including records stored on backup media, in a form that includes the complete record. You also are requested not to disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. **If compliance with this request may result in a permanent or temporary termination of service to the accounts described below, or otherwise alert the subscriber or user of these accounts as to your actions to preserve the referenced files and records, please contact me before taking such actions.**

This request applies only retrospectively. It does not in any way obligate you to capture and preserve new information that arises after the date of this request.

This preservation request applies to the following records and evidence:

[In a case involving an e-mail account]

A. All stored electronic communications and other files reflecting communications to or from the following electronic mail address:
[JDoe@isp.com];

B. All records and other evidence relating to the subscriber(s), customer(s), account holder(s), or other entity(ies) associated with the e-mail address **[JDoe@isp.com]** or user name "Jdoe," including, without limitation, subscriber names, user names, screen names or other identities, mailing addresses, residential addresses, business addresses, e-mail addresses and other contact information, telephone numbers or other subscriber number or identity, billing records, information about the length of service and the types of services the subscriber or

customer utilized, and any other identifying information, whether such records or other evidence are in electronic or other form; and

C. Any other records and other evidence relating to the e-mail address

[JDoe@isp.com] or user name "Jdoe." Such records and other evidence include, without limitation, correspondence and other records of contact by any person or entity about the above-referenced account, the content and connection logs associated with user activity or relating to communications and any other activities to, through or from **[JDoe@isp.com]** or user name "Jdoe," whether such records or other evidence are in electronic or other form.

[In a case involving use of a specific I.P. address]

All electronic records and other evidence relating to the use of the IP address 222.222.222.2 or domain name abc.wcom.net on September 5, 1999 at 4:28 and 04:32 GMT +02:00, and on September 7, 1999 at 00:19 GMT +02:00.

[In a case involving activity of a user account]

All connection logs and records of user activity for the user name **Jdoe** or address **[JDoe@isp.com]**, including:

1. Connection date and time;
2. Disconnect date and time;
3. Method of connection (e.g., telnet, ftp, http);
4. Data transfer volume;
5. User name associated with the connection and other connection information, including the Internet Protocol address of the source of the connection;
6. Telephone caller identification records; and
7. Connection information for other computers to which the user of the above-referenced accounts connected, by any means, during the connection period, including the destination IP address, connection time and date, disconnect time and date, method of connection to the destination computer, the identities (account and screen names) and subscriber information, if known, for any person or entity to which such connection information relates, and all other information related to the connection from ISP or its subsidiaries.

All records and other evidence relating to the subscriber(s), customer(s), account holder(s), or other entity(ies) associated with **[JDoe@isp.com]**, including, without limitation, subscriber names, user names, screen names or other identities, mailing addresses, residential addresses, business addresses, e-mail addresses and other contact information, telephone numbers or other subscriber number or identifier number, billing records, information about the length of service and the types of services the subscriber or customer utilized, and any other identifying information, whether such records or other evidence are in electronic or other form.

Any other records and other evidence relating to **[JDoe@isp.com]**. Such records and other evidence include, without limitation, correspondence and other records of contact by any person or entity about the above-referenced account, the content and connection logs associated with or relating to postings, communications and any other activities to or through **[JDoe@isp.com]**, whether such records or other evidence are in electronic or other form.

Very truly yours,

Assistant United States Attorney

**Appendix D: Sample Pen Register /Trap
and Trace Application and Order**

UNITED STATES DISTRICT COURT
FOR THE _____ DISTRICT OF _____

IN RE APPLICATION OF THE)	
UNITED STATES OF AMERICA FOR)	MISC. NO. _____
AN ORDER AUTHORIZING THE USE)	
OF A PEN REGISTER AND TRAP AND)	Filed Under Seal
TRACE DEVICE)	

APPLICATION

[Name], an Assistant United States Attorney for the _____ District of _____, hereby files under seal this ex parte application for an Order under Title 18, United States Code, Section 3123, authorizing the installation and use of a pen/trap device on a computer operated by [Internet Service Provider]. This computer is named [computer name], has an IP address of [IP address], and is believed to be located at [physical address]. In support of this application, the undersigned states the following:

1. Applicant is an “attorney for the government” as defined in Rule 54(c) of the Federal Rules of Criminal Procedure and, therefore, pursuant to Section 3122 of Title 18, United States Code, may apply for an order authorizing the installation and use of a pen/trap device.

2. Applicant certifies that the Federal Bureau of Investigations is conducting a criminal investigation of [suspect] and others yet unknown in connection with possible violations of Title 18 United States Code, Section [], to wit, [statutory description of offense]. It is believed the subject(s) of the investigation may be using the electronic mail address [JDoe@isp.com], in furtherance of the specified offense, and that the information likely to be obtained from the pen/trap device is relevant to the ongoing criminal investigation. **[Although not required by law, CCIPS recommends the**

inclusion within the application of specific and articulable facts that support this conclusion.]

3. A trap and trace device, as defined in Title 18, United States Code, Section 3127, is “a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted.” A pen register collects destination information for electronic transmissions. In the traditional telephone context, a pen register and trap and trace device collects origin and destination information such as the telephone numbers dialed for a telephone call. The same principles apply in the context of Internet communications: a pen register and trap and trace device collects addressing information contained in “packet headers,” and, in the case of e-mails, “mail headers.” Both “packet headers” and “mail headers” are portions of Internet communications that contain addressing information, analogous to “to” and “from” addresses for traditional letters and origin and destination telephone numbers for telephone calls. Importantly, “packet headers” and “mail headers” (minus the subject lines of e-mails, which contain the e-mails’ titles and can include messages) do not contain the contents of electronic communications. Accordingly, this application does not seek authority to intercept the contents of any electronic communications. To obtain the contents of electronic communications in transmission (including the subject lines of e-mails), the government ordinarily must apply for and receive a Title III order pursuant to 18 U.S.C. §§ 2510-22. Because the “to” and “from” information contained within packet headers and mail headers can be obtained through the same combination of software and hardware, this application and order refers to means of obtaining both the origination and destination information as simply a “pen/trap” device.

4. Applicant requests that the Court issue an Order authorizing the installation and use of a pen/trap device to capture the packet header and mail header information (but not the subject lines of e-mails) associated with the transmission of communications and other data (including transfers of information via the World Wide Web, electronic mail,

telnet, and the file transfer protocol) to and from the account [Jdoe@isp.com]; to record the date and time of the initiation and receipt of such transmissions; and to record the length of time the transmissions took place, all for a period of sixty (60) days following installation.

5. The Applicant further requests that the Order direct the furnishings of information, facilities, and technical assistance necessary to accomplish the installation of the pen/trap device unobtrusively by [Internet Service Provider], with reasonable compensation to be paid by the applicant for reasonable expenses incurred in providing such facilities and assistance.

WHEREFORE, it is respectfully requested that the Court grant an Order for a period of sixty (60) days (1) authorizing the installation and use of a pen/trap device to capture the packet header and mail header information (but not the subject lines of e-mails) associated with all communications and other data transmitted to or from the account [JDoe@isp.com]; to record the date and time of such transmissions; and to record the length of time the transmission took; (2) directing [Internet Service Provider] to furnish the Federal Bureau of Investigations, forthwith, all information, facilities, and technical assistance necessary to accomplish the installation and use of the device unobtrusively and with a minimum of interference to the service presently accorded persons whose transmissions are the subject of the pen/trap device; and (3) that this Application and Order be placed under seal and further direct that [Internet Service Provider], and its agents and employees, not disclose to the listed subscriber, or to any other person, the existence of the pen/trap device or of this investigation unless or until otherwise ordered by the Court.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on _____.

Respectfully Submitted,

Assistant United States Attorney

UNITED STATES DISTRICT COURT
FOR THE _____ DISTRICT OF _____

IN RE APPLICATION OF THE)	
UNITED STATES OF AMERICA FOR)	MISC. NO. _____
AN ORDER AUTHORIZING THE USE)	
OF A PEN REGISTER AND TRAP AND)	Filed Under Seal
TRACE DEVICE)	

ORDER

This matter having come before the Court pursuant to an Application under Title 18, United States Code, Section 3122, by [Name], Assistant United States Attorney, _____ District of _____, which Application requests an Order under Title 18, United States Code, Section 3123, authorizing the installation and use of a pen/trap device on the account [JDoe@isp.com], the Court finds that the applicant has certified that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation into possible violations of Title 18, United States Code, Section _____, to wit, [statutory description of offense] by [suspect], and others yet unknown.

IT APPEARING that the packet header and mail header information associated with communications and other data transmitted to and from the account [JDoe@isp.com] are relevant to an ongoing criminal investigation of the specified offense;

IT IS ORDERED, pursuant to Title 18, United States Code, Section 3123, that agents of the Federal Bureau of Investigations may install and use a pen/trap device to capture the packet header and mail header information (but not the subject lines of e-mails) for all communications and other data transmitted to and from the account [Jdoe@isp.com]; to record the date and time of such transmissions; and to record the length of time the transmissions took, for a period of sixty (60) days from the date of this Order;

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3123(b)(2), that [Internet Service Provider] shall furnish agents of the Federal Bureau of

Investigations, forthwith, all information, facilities, and technical assistance necessary to accomplish the installation and use of the pen/trap device unobtrusively and with minimum interference to the services that are accorded persons with respect to whom the installation and use is to take place;

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3123(d), that this Order and the Application be sealed until otherwise ordered by the Court, and that copies of such order may be furnished to the Federal Bureau of Investigations, United States Attorney's Office, and [Internet Service Provider], and further that [Internet Service Provider] shall not disclose the existence of the pen/trap device or the existence of the investigation to the listed subscriber or to any other person unless or until otherwise ordered by the Court.

United States Magistrate Judge

Date

Appendix E: Sample Subpoena Language

The following is sample language for obtaining basic subscriber information with a subpoena pursuant to 18 U.S.C. § 2703(c)(1)(C):

All customer or subscriber account information for any accounts registered to _____, or associated with _____. For each such account, the information shall include:

1. *The subscriber's name;*
2. *The subscriber's address;*
3. *The subscriber's local and long distance telephone toll billing records*
4. *The subscriber's telephone number or numbers, the e-mail address or _____ addresses,*
5. *The types of services subscribed to or utilized by the subscriber and the lengths of such services.*

The following is sample language for obtaining the content of communications when permitted by ECPA pursuant to 18 U.S.C. § 2703(a) and (b):

3. The contents of electronic communications not in "electronic storage" (i.e., electronic mail that has already been opened by the user) currently held or maintained in the account associated with the address "____@____" (registered to _____) sent from or to the above account during the period _____ through _____ (inclusive).
2. The content of all electronic communications in "electronic storage" for more than 180 days associated with the accounts identified in Part A, that were placed or stored in _____ computer systems in directories or files owned or controlled by such accounts at any time up through and including the date of this subpoena.

[ISP] should NOT produce any unopened incoming electronic communications (i.e., electronic communications in "electronic storage") less than 181 days old.

For purposes of this request, "electronic storage" is defined in 18 U.S.C. § 2510(17) as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication." The government does not seek access to any such materials, unless it has been in storage for more than 180 days.

Appendix F: Sample Language for Search Warrants and Accompanying Affidavits to Search and Seize Computers

This appendix provides sample language for agents and prosecutors who wish to obtain a warrant authorizing the search and seizure of computers. The discussion focuses first on the proper way to describe the property to be seized in the warrant itself, which in turn requires consideration of the role of the computer in the offense. The discussion then turns to drafting an accompanying affidavit that establishes probable cause, describes the agent's search strategy, and addresses any additional statutory or constitutional concerns.

1. DESCRIBING THE PROPERTY TO BE SEIZED FOR THE WARRANT

The first step in drafting a warrant to search and seize computers or computer data is to describe the property to be seized for the warrant itself. This requires a particularized description of the evidence, contraband, fruits, or instrumentality of crime that the agents hope to obtain by conducting the search.

Whether the 'property to be seized' should contain a description of information (such as computer files) or physical computer hardware depends on the role of the computer in the offense. In some cases, the computer hardware is itself contraband, evidence of crime, or a fruit or instrumentality of crime. In these situations, Fed. R. Crim. P. 41 expressly authorizes the seizure of the hardware, and the warrant will ordinarily request its seizure. In other cases, however, the computer hardware is merely a storage device for electronic files that are themselves contraband, evidence, or instrumentalities of crime. In these cases, the warrant should request authority to search for and seize the information itself, not the storage devices that the agents believe they must seize to recover the information. Although the agents may need to seize the storage devices for practical reasons, such practical considerations are best addressed in the accompanying affidavit. The 'property to be seized' described in the warrant should fall within one or more of the categories listed in Rule 41(b):

(1) "property that constitutes evidence of the commission of a criminal offense"

This authorization is a broad one, covering any item that an investigator "reasonably could . . . believe" would reveal information that would aid in a particular apprehension or conviction. Andresen v. Maryland, 427 U.S. 463, 483 (1976). Cf. Warden v. Hayden, 387 U.S. 294, 307 (1967) (noting that restrictions on what evidence may be seized result mostly from the probable cause requirement). The word "property" in Rule 41(b)(1) includes both tangible and intangible property. See United States v. New York Tel. Co., 434 U.S. 159, 169 (1977) ("Rule 41 is not limited to tangible items but is sufficiently flexible to include within its scope electronic intrusions authorized

upon a finding of probable cause.”); United States v. Biasucci, 786 F.2d 504, 509-10 (2d Cir. 1986) (holding that the fruits of video surveillance are “property” that may be seized using a Rule 41 search warrant). Accordingly, data stored in electronic form is “property” that may properly be searched and seized using a Rule 41 warrant. See United States v. Hall, 583 F. Supp. 717, 718-19 (E.D. Va. 1984).

(2) *“contraband, the fruits of crime, or things otherwise criminally possessed”*

Property is contraband “when a valid exercise of the police power renders possession of the property by the accused unlawful and provides that it may be taken.” Hayden, 387 U.S. at 302 (quoting Gouled v. United States, 255 U.S. 298, 309 (1921)). Common examples of items that fall within this definition include child pornography, see United States v. Kimbrough, 69 F.3d 723, 731 (5th Cir. 1995), pirated software and other copyrighted materials, see United States v. Vastola, 670 F. Supp. 1244, 1273 (D.N.J. 1987), counterfeit money, narcotics, and illegal weapons. The phrase “fruits of crime” refers to property that criminals have acquired as a result of their criminal activities. Common examples include money obtained from illegal transactions, see United States v. Dornblut, 261 F.2d 949, 951 (2d Cir. 1958) (cash obtained in drug transaction), and stolen goods. See United States v. Burkeen, 350 F.2d 261, 264 (6th Cir. 1965) (currency removed from bank during bank robbery).

(3) *“property designed or intended for use or which is or had been used as a means of committing a criminal offense”*

Rule 41(b)(3) authorizes the search and seizure of “property designed or intended for use or which is or had been used as a means of committing a criminal offense.” This language permits courts to issue warrants to search and seize instrumentalities of crime. See United States v. Farrell, 606 F.2d 1341, 1347 (D.C. Cir. 1979). Computers may serve as instrumentalities of crime in many ways. For example, Rule 41 authorizes the seizure of computer equipment as an instrumentality when a suspect uses a computer to view, acquire, and transmit images of child pornography. See Davis v. Gracey, 111 F.3d 1472, 1480 (10th Cir. 1997) (stating in an obscenity case that “the computer equipment was more than merely a ‘container’ for the files; it was an instrumentality of the crime.”); United States v. Lamb, 945 F. Supp. 441, 462 (N.D.N.Y. 1996). Similarly, a hacker’s computer may be used as an instrumentality of crime, and a computer used to run an illegal Internet gambling business would also be an instrumentality of the crime.

Here are examples of how to describe property to be seized when the computer hardware is merely a storage container for electronic evidence:

- (1) *All records relating to violations of 21 U.S.C. § 841(a) (drug trafficking) and/or 21 U.S.C. § 846 (conspiracy to traffic drugs) involving [the suspect] since January 1, 1996, including*

lists of customers and related identifying information; types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions; any information related to sources of narcotic drugs (including names, addresses, phone numbers, or any other identifying information); any information recording [the suspect's] schedule or travel from 1995 to the present; all bank records, checks, credit card bills, account information, and other financial records.

The terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any electrical, electronic, or magnetic form (such as any information on an electronic or magnetic storage device, including floppy diskettes, hard disks, ZIP disks, CD-ROMs, optical discs, backup tapes, printer buffers, smart cards, memory calculators, pagers, personal digital assistants such as Palm Pilot computers, as well as printouts or readouts from any magnetic storage device); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies).

- (2) *Any copy of the X Company's confidential May 17, 1998 report, in electronic or other form, including any recognizable portion or summary of the contents of that report.*

- (3) *[For a warrant to obtain records stored with an ISP pursuant to 18 U.S.C. Section 2703(a)] All stored electronic mail of any kind sent to, from and through the e-mail address [JDoe@isp.com], or associated with the user name "John Doe," or account holder [suspect]. Content and connection log files of all account activity from January 1, 2000, through March 31, 2000, by the user associated with the e-mail address [JDoe@isp.com], including dates, times, methods of connecting (e.g., telnet, ftp, http), ports used, telephone dial-up caller identification records, and any other connection information or traffic data. All business records, in any form kept, in the possession of [Internet Service Provider], that pertain to the subscriber(s) and account(s) associated with the e-mail address [JDoe@isp.com], including records showing the subscriber's full name, all screen names associated with that subscriber and account, all account names associated with that subscriber, methods of payment, phone numbers, all residential, business, mailing, and e-mail addresses, detailed billing records, types and lengths of service, and any other identifying information.*

Here are examples of how to describe the property to be seized when the computer hardware itself is evidence, contraband, or an instrumentality of crime:

- (1) *Any computers (including file servers, desktop computers, laptop computers, mainframe computers, and storage devices such as hard drives, Zip disks, and*

floppy disks) that were or may have been used as a means to provide images of child pornography over the Internet in violation of 18 U.S.C. § 2252A that were accessible via the World Wide Website address www.[xxxxxxx].com.

(2) *IBM Thinkpad Model 760ED laptop computer with a black case*

2. DRAFTING AFFIDAVITS IN SUPPORT OF WARRANTS TO SEARCH AND SEIZE COMPUTERS

An affidavit to justify the search and seizure of computer hardware and/or files should include, at a minimum, the following sections: (1) definitions of any technical terms used in the affidavit or warrant; (2) a summary of the offense, and, if known, the role that a targeted computer plays in the offense; and (3) an explanation of the agents' search strategy. In addition, warrants that raise special issues (such as sneak-and-peek warrants, or warrants that may implicate the Privacy Protection Act, 42 U.S.C. § 2000aa) require thorough discussion of those issues in the affidavit. Agents and prosecutors with questions about how to tailor an affidavit and warrant for a computer-related search may contact either the local CTC, or the Computer Crime & Intellectual Property Section at (202) 514-1026.

3. Background Technical Information

It may be helpful to include a section near the beginning of the affidavit explaining any technical terms that the affiant may use. Although many judges are computer literate, judges generally appreciate a clear, jargon-free explanation of technical terms that may help them understand the merits of the warrant application. At the same time, agents and prosecutors should resist the urge to pad affidavits with long, boilerplate descriptions of well-known technical phrases. As a rule, affidavits should only include the definitions of terms that are likely to be unknown by a generalist judge and are used in the remainder of the affidavit. Here are several sample definitions:

Encryption

Encryption refers to the practice of mathematically scrambling computer data as a communications security measure. The encrypted information is called "ciphertext." "Decryption" is the process of converting the ciphertext back into the original, readable information (known as "plaintext"). The word, number or other value used to encrypt/decrypt a message is called the "key."

Data Compression

A process of reducing the number of bits required to represent some information, usually to reduce the time or cost of storing or transmitting it. Some methods can be reversed to reconstruct the original data exactly; these are used for faxes, programs and most computer data. Other methods do not exactly reproduce the original data, but this may be acceptable (for example, for a video conference).

Joint Photographic Experts Group (JPEG)

JPEG is the name of a standard for compressing digitized images that can be stored on computers. JPEG is often used to compress photographic images, including pornography. Such files are often identified by the ".jpg" extension (such that a JPEG file might have the title "picture.jpg") but can easily be renamed without the ".jpg" extension.

Internet Service Providers ("ISPs")

Many individuals and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP.

ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data format and in written record format.

ISPs reserve and/or maintain computer disk storage space on their computer system for the use of the Internet service subscriber for both temporary and long-term storage of electronic communications with other parties and other types of electronic data and files. E-mail that has not been opened is stored temporarily by an ISP incident to the transmission of the e-mail to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as "electronic storage," and the provider of such a service is an "electronic communications service" provider. A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long term storage services to the public for electronic data and files, is providing a "remote computing service."

Server

A server is a centralized computer that provides services for other computers connected to it via a network. The other computers attached to a server are sometimes called "clients." In a large company, it is common for individual employees to have client computers at their desktops. When the employees access their e-mail, or access files stored on the network itself, those files are pulled electronically from the server, where they are stored, and are sent to the client's computer via the network. Notably, server computers can be physically stored in any location: it is common for a network's server to be located hundreds (and even thousands) of miles away from the client computers.

In larger networks, it is common for servers to be dedicated to a single task. For example, a server that is configured so that its sole task is to support a World Wide Web site is known simply as a "web server." Similarly, a server that only stores and processes e-mail is known as a "mail server."

IP Address

The Internet Protocol address (or simply "IP" address) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses.

dynamic IP address When an ISP or other provider uses dynamic IP addresses, the ISP randomly assigns one of the available IP addresses in the range of IP addresses controlled by the ISP each time a user dials into the ISP to connect to the Internet. The customer's computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that period. Once the user disconnects, however, that IP address becomes available to other customers who dial in at a later time. Thus, an individual customer's IP address normally differs each time he dials into the ISP.

static IP address A static IP address is an IP address that is assigned permanently to a given user or computer on a network. A customer of an ISP that assigns static IP addresses will have the same IP address every time.

B. Describe the Role of the Computer in the Offense

The next step is to describe the role of the computer in the offense, to the extent it is known. For example, is the computer hardware itself evidence of a crime or contraband? Is the computer hardware merely a storage device that may or may not contain electronic files that constitute evidence of a crime? To introduce this topic, it may be helpful to explain at the outset why the role of the computer is important for defining the scope of your warrant request.

Your affiant knows that computer hardware, software, and electronic files may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of crime, contraband, instrumentalities of crime, and/or fruits of crime. In this case, the warrant application requests permission to search and seize [images of child pornography, including those that may be stored on a computer]. These [images] constitute both evidence of crime and contraband. This affidavit also requests permission to seize the computer hardware that may contain [the images of child pornography] if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. Your affiant believes that, in this case, the computer hardware is a container for evidence, a container for contraband, and also itself an instrumentality of the crime under investigation.

1. When the Computer Hardware Is Itself Contraband, Evidence, And/or an Instrumentality or Fruit of Crime

If applicable, the affidavit should explain why probable cause exists to believe that the tangible computer items are themselves contraband, evidence, instrumentalities, or fruits of the crime, independent of the information they may hold.

Computer Used to Obtain Unauthorized Access to a Computer (“Hacking”)

Your affiant knows that when an individual uses a computer to obtain unauthorized access to a victim computer over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage device for evidence of the

crime. The computer is an instrumentality of the crime because it is "used as a means of committing [the] criminal offense" according to Rule 41(b)(3). In particular, the individual's computer is the primary means for accessing the Internet, communicating with the victim computer, and ultimately obtaining the unauthorized access that is prohibited by 18 U.S.C. § 1030. The computer is also likely to be a storage device for evidence of crime because computer hackers generally maintain records and evidence relating to their crimes on their computers. Those records and evidence may include files that recorded the unauthorized access, stolen passwords and other information downloaded from the victim computer, the individual's notes as to how the access was achieved, records of Internet chat discussions about the crime, and other records that indicate the scope of the individual's unauthorized access.

Computers Used to Produce Child Pornography

It is common for child pornographers to use personal computers to produce both still and moving images. For example, a computer can be connected to a common video camera using a device called a video capture board: the device turns the video output into a form that is usable by computer programs. Alternatively, the pornographer can use a digital camera to take photographs or videos and load them directly onto the computer. The output of the camera can be stored, transferred or printed out directly from the computer. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. All of these devices, as well as the computer, constitute instrumentalities of the crime.

2. When the Computer Is Merely a Storage Device for Contraband, Evidence, And/or an Instrumentality or Fruit of Crime

When the computer is merely a storage device for electronic evidence, the affidavit should explain this clearly. The affidavit should explain why there is probable cause to believe that evidence of a crime may be found in the location to be searched. This does not require the affidavit to establish probable cause that the evidence may be stored specifically within a computer. However, the affidavit should explain why the agents believe that the information may in fact be stored as an electronic file stored in a computer.

Child Pornography

Your affiant knows that child pornographers generally prefer to store images of child pornography in electronic form as computer files. The computer's ability to store images in digital form makes a computer an ideal repository for pornography. A small portable disk can contain hundreds or thousands of images of child pornography, and a computer hard drive can contain tens of thousands of such images at very high resolution. The images can be easily sent to or received from other computer users over the Internet. Further, both individual files of child pornography and the disks that contain the files can be mislabeled or hidden to evade detection.

Illegal Business Operations

Based on actual inspection of [spreadsheets, financial records, invoices], your affiant is aware that computer equipment was used to generate, store, and print documents used in [suspect's] [tax evasion, money laundering, drug trafficking, etc.] scheme. There is reason to believe that the computer system currently located on [suspect's] premises is the same system used to produce and store the [spreadsheets, financial records, invoices], and that both the [spreadsheets, financial records, invoices] and other records relating to [suspect's] criminal enterprise will be stored on [suspect's computer].

C. The Search Strategy

The affidavit should also contain a careful explanation of the agents' search strategy, as well as a discussion of any practical or legal concerns that govern how the search will be executed. Such an explanation is particularly important when practical considerations may require that agents seize computer hardware and search it off-site when that hardware is only a storage device for evidence of crime. Similarly, searches for computer evidence in sensitive environments (such as functioning businesses) may require that the agents adopt an incremental approach designed to minimize the intrusiveness of the search. The affidavit should explain the agents' approach in sufficient detail that the explanation provides a useful guide for the search team and any reviewing court. It is a good practice to include a copy of the search strategy as an attachment to the warrant, especially when the affidavit is placed under seal. Here is sample language that can apply recurring situations:

1. Sample Language to Justify Seizing Hardware and Conducting a Subsequent Off-site Search

Based upon your affiant's knowledge, training and experience, your affiant knows that searching and seizing information from computers often requires agents to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

(1) The volume of evidence. Computer storage devices (like hard disks, diskettes, tapes, laser disks) can store the equivalent of millions of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

(2) Technical Requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis. Further, such searches often require the seizure of most or all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment.

In light of these concerns, your affiant hereby requests the Court's permission to seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence.

2. Sample Language to Justify an Incremental Search

Your affiant recognizes that the [Suspect] Corporation is a functioning company with approximately [number] employees, and that a seizure of the [Suspect] Corporation's computer network may have the unintended and undesired effect of limiting the company's ability to provide service to its legitimate customers who are not engaged in [the criminal activity under investigation]. In response to these concerns, the agents who execute the search will take an incremental approach to minimize the inconvenience to [Suspect Corporation]'s legitimate customers and to minimize the need to seize equipment and data. This incremental approach, which will be explained to all of the agents on the search team before the search is executed, will proceed as follows:

A. Upon arriving at the [Suspect Corporation's] headquarters on the morning of the search, the agents will attempt to identify a system administrator of the network (or other knowledgeable employee) who will be willing to assist law enforcement by identifying, copying, and printing out paper [and electronic] copies of [the computer files described in the warrant.] If the agents succeed at locating such an employee and are able to obtain copies of the [the computer files described in the warrant] in that way, the agents will not conduct any additional search or seizure of the [Suspect Corporation's] computers.

B. If the employees choose not to assist the agents and the agents cannot execute the warrant successfully without themselves examining the [Suspect Corporation's] computers, primary responsibility for the search will transfer from the case agent to a designated computer expert. The computer expert will attempt to locate [the computer files described in the warrant], and will attempt to make electronic copies of those files. This analysis will focus on particular programs, directories, and files that are most likely to contain the evidence and information of the violations under investigation. The computer expert will make every effort to review and copy only those programs, directories, files, and materials that are evidence of the offenses described herein, and provide only those items to the case agent. If the computer expert succeeds at locating [the computer files described in the warrant] in that way, the agents will not conduct any additional search or seizure of the [Suspect Corporation's] computers.

C. If the computer expert is not able to locate the files on-site, or an on-site search proves infeasible for technical reasons, the computer expert will attempt to create an electronic "image" of those parts of the computer that

are likely to store [the computer files described in the warrant]. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Imaging a computer permits the agents to obtain an exact copy of the computer's stored data without actually seizing the computer hardware. The computer expert or another technical expert will then conduct an off-site search for [the computer files described in the warrant] from the "mirror image" copy at a later date. If the computer expert successfully images the [Suspect Corporation's] computers, the agents will not conduct any additional search or seizure of the [Suspect Corporation's] computers.

D. If "imaging" proves impractical, or even impossible for technical reasons, then the agents will seize those components of the [Suspect Corporation's] computer system that the computer expert believes must be seized to permit the agents to locate [the computer files described in the warrant] at an off-site location. The components will be seized and taken in to the custody of the FBI. If employees of [Suspect Corporation] so request, the computer expert will, to the extent practicable, attempt to provide the employees with copies of any files [not within the scope of the warrant] that may be necessary or important to the continuing function of the [Suspect Corporation's] legitimate business. If, after inspecting the computers, the analyst determines that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it within a reasonable time.

3. Sample Language to Justify the Use of Comprehensive Data Analysis Techniques

Searching [the suspect's] computer system for the evidence described in [Attachment A] may require a range of data analysis techniques. In some cases, it is possible for agents to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, agents may be able to execute a "keyword" search that searches through the files stored in a computer for special words that are likely to appear only in the materials covered by a warrant. Similarly, agents may be able to locate the materials covered in the warrant by looking for particular directory or file names. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files and directories; encode communications to avoid using key words; attempt to delete files to evade detection; or take other steps designed to frustrate law enforcement searches for

information. These steps may require agents to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or opening every file and scanning its contents briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in [Attachment A].

4. Special Considerations

The affidavit should also contain discussions of any special legal considerations that may factor into the search or how it will be conducted. These considerations are discussed at length in Chapter 2. Agents can use this checklist to determine whether a particular computer-related search raises such issues:

1. **Is the search likely to result in the seizure of any drafts of publications (such as books, newsletters, Web site postings, etc.) that are unrelated to the search and are stored on the target computer?** If so, the search may implicate the Privacy Protection Act, 42 U.S.C. § 2000aa.
2. **Is the target of the search an ISP, or will the search result in the seizure of a mail server?** If so, the search may implicate the Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-11.
3. **Does the target store electronic files or e-mail on a server maintained in a remote location?** If so, the agents may need to obtain more than one warrant.
4. **Will the search result in the seizure of privileged files, such as attorney-client communications?** If so, special precautions may be in order.
5. **Are the agents requesting authority to execute a sneak-and-peek search?**
6. **Are the agents requesting authority to dispense with the “knock and announce” rule?**

Appendix G: Sample Letter for Provider Monitoring

This letter is intended to inform [law enforcement agency] of [Provider's] decision to conduct monitoring of unauthorized activity within its computer network pursuant to 18 U.S.C. § 2511(2)(a)(i), and to disclose some or all of the fruits of this monitoring to law enforcement if [Provider] deems it will assist in protecting its rights or property. On or about [date], [Provider] became aware that it was the victim of unauthorized intrusions into its computer network. [Provider] understands that 18 U.S.C. § 2511(2)(a)(i) authorizes

an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service[.]

This statutory authority permits [Provider] to engage in reasonable monitoring of unauthorized use of its network to protect its rights or property, and also to disclose intercepted communications to [law enforcement] to further the protection of [Provider]'s rights or property.

To protect its rights and property, [Provider] plans to [continue to] conduct reasonable monitoring of the unauthorized use in an effort to evaluate the scope of the unauthorized activity and attempt to discover the identity of the person or persons responsible. [Provider] may then wish to disclose some or all of the fruits of its interception to law enforcement to help support a criminal investigation concerning the unauthorized use and criminal prosecution for the unauthorized activity of the person(s) responsible.

[Provider] understands that it is under absolutely no obligation to conduct any monitoring whatsoever, or to disclose the fruits of any monitoring, and that 18 U.S.C. § 2511(2)(a)(i) does not permit [law enforcement] to direct or request [Provider] to intercept, disclose, or use monitored communications for law enforcement purposes. Accordingly, [law enforcement] will under no circumstances initiate, encourage, order, request, or solicit [Provider] to conduct nonconsensual monitoring without first obtaining an appropriate court order, and [Provider] will not engage in monitoring solely or primarily to assist law enforcement absent an appropriate court order. Any monitoring and/or disclosure will be at [Provider's] initiative. [Provider] also recognizes that the interception of wire and electronic communications beyond the permissible scope of 18 U.S.C. § 2511(2)(a)(i) potentially may subject it to civil and criminal penalties.

Sincerely,
[Provider] General Counsel

INDEX

<u>Topic</u>	<u>Chapter</u>
Banners	
and Reasonable Expectation of Privacy	(1)(d)(2)(a)
and Title III	(4)(c)(3)(b)(i)
Sample Language	Appendix A
Border Searches	(1)(c)(6)
Consent, Fourth Amendment	
Generally	(1)(c)(1)
Implied Consent	(1)(c)(1)(c)
Scope of Consent	(1)(c)(1)(a)
Third Party	
Generally	(1)(c)(1)(b)
Parents	(1)(c)(1)(b)(iii)
Private Sector Workplaces	(1)(d)(1)(b)
Public Sector Workplaces	(1)(d)(2)(c)
Spouses and Domestic Partners	(1)(c)(1)(b)(ii)
System Administrators	(1)(c)(1)(b)(iv)
Consent, Statutory	
ECPA	(3)(e)
Title III	(4)(c)(3)(b)
Drafting Warrants, <u>see</u> Warrants	
ECPA (18 U.S.C. §§ 2701-2711)	
Generally	(3)
2703(d) Orders	(3)(d)(3)(d)(iv)
2703(f) Letters	(3)(g)(1)
and The Cable Act	(3)(g)(3)
Basic Subscriber Information	(3)(c)(1)(e)(ii)
Consent of System Administrator	(1)(c)(1)(b)(iv)
Contents	(3)(c)(3)(e)(i)
Electronic Communication Service	(3)(b)
Electronic Storage	(3)(b)
Non-Disclosure Letters	(3)(g)(2)
Remote Computing Service	(3)(b)
Quick Reference Guide	(3)(f)

Remedies	(3)(h)
Sample Applications and Orders	Appendices
Search Warrants	(3)(d)(5)
and Search and Seizure	(2)(a)(2)(b)(iii)
Subpoenas	(3)(d)(1),
	(3)(d)(2)
Transactional Records	(3)(c)(2)
Exceptions to Warrant Requirement	(1)(c)
<u>see</u> Border Searches; Consent;	
Exigent Circumstances;	
Inventory Searches; Plain View;	
Search Incident to Lawful Arrest;	
O'Connor v. Ortega Workplace Searches	
Exigent Circumstances	(1)(c)(2)
Evidence	
Generally	(5)
Authentication	(5)(b)
Business Records	(5)(a)
	(5)(c)(2)
Hearsay	(5)(c)
“Flagrant Disregard” Test	(2)(c)(3)
Fourth Amendment	
Warrantless Searches	(1)
Warrant Searches, <u>see also</u> Warrants	(2)
Good Faith Defense	
Execution of Search Warrants	(2)(c)(3)
Violations of Title III	(4)(d)(2)(a)
International Issues	
Generally	(1)(c)(7)
Remote Searches and Rule 41	(2)(b)(4)
Inventory Searches	(1)(c)(5)
Multiple Warrants, <u>see</u> Warrants	
No-Knock Warrants, <u>see</u> Warrants	

O'Connor v. Ortega Workplace Searches	(1)(d)(2)(b)
Off-site vs. On-site Searches	(2)(b)(1)
Pagers	
Reasonable Expectation of Privacy	(1)(b)(2)
Exigent Circumstances	(1)(c)(2)
Search Incident to a Lawful Arrest	(1)(c)(4)
Particularity, Search Warrant	(2)(c)(3)
Pen Registers and Trap and Trace Devices (18 U.S.C. §§ 3121-3127)	
Generally	(4)(b)
Remedies	(4)(d)
and Title III	(4)(a)
Sample Application and Order	Appendix D
Planning a Search	(2)(b)
Plain View	(1)(c)(3)
Privacy Protection Act ("PPA"), 42 U.S.C. § 2000aa	
Application to Computer Cases	(2)(b)(2)(c)
Generally	(2)(b)(1)(a)
History	(2)(b)(2)(a)
And Planning a Search	(2)(a)(2)
Statutory Language	(2)(b)(2)(b)
Private Searches	
Generally	(1)(b)(4)
Private Employers	(1)(d)(1)(c)
Privileged Documents	
Generally	(2)(b)(7)
Regulations	(2)(b)(7)(a)
Reviewing Privileged Materials	(2)(b)(7)(b)
Probable Cause	(2)(c)(1)
Qualified Immunity, <i>see</i> Title III	
Reasonable Expectation of Privacy	
Generally	(1)(b)(1)

Computers as Storage Devices and ECPA in Private Sector Workplaces in Public Sector Workplaces and Third Party Possession and Title III for Computer Hackers	(1)(b)(2) (3)(a) (1)(d)(1)(a) (1)(d)(2)(a) (1)(b)(3) (4)(d)(1)(b) (4)(d)(1)(a)(ii)
Remedies	
ECPA	(3)(h)
Pen/Trap Devices	(4)(d)
Rule 41	(2)(b)(4), (2)(b)(6)
Title III	(4)(d)
Rule 41	
Generally and “Flagrant Disregard”	(2)(b)(1) (2)(c)(2)
Rule 41(a)	(2)(b)(4)
Rule 41(d)	(2)(b)(6)
Rule 41(e)	(2)(d)(2), (2)(d)(3)
Seizure	
Temporary of Hardware, vs. Searching On-site	(1)(b)(4) (2)(b)(1)
Search Incident to a Lawful Arrest	(1)(c)(4)
Search Warrants, <u>see</u> Warrants	
Sneak and Peek Warrants, <u>see</u> Warrants	
Subpoenas	
and ECPA	(3)(d)(1) (3)(d)(2)
Sample language	Appendix E
Suppression, <u>see</u> Remedies	
Surveillance, <u>see</u> Pen Registers and Trap and Trace Devices, Title III	
Title III (18 U.S.C. §§ 2510-2522)	
Generally	(4)(c)
Banners	(4)(c)(3)(b)(i)

Consent Exception	(4)(c)(3)(b)
Electronic Communication	(4)(c)(2)
Extension Telephone Exception	(4)(c)(3)(d)
Intercept	(4)(c)(2)
Provider Exception	(4)(c)(3)(c)
Remedies	(4)(d)
Good Faith Defense	(4)(d)(2)(a)
Qualified Immunity	(4)(d)(2)(b)
Suppression	(4)(d)(1)
Wire Communication	(4)(c)(2)
Trap and Trace Devices, <u>see</u> Pen Registers and Trap and Trace Devices	
2703(d) Orders	
Legal Requirements	(3)(d)(3)
Sample Application and Order	Appendix B
Voice Mail	(3)(d)
Warrants	
Generally	(2)
for Computers in Law Enforcement Custody	(2)(d)(1)
Drafting	(2)(c)
under ECPA	(3)(d)(5)
General Strategies	(2)(a)
Multiple	(2)(b)(4)
No-Knock	(2)(b)(5)
Planning a Search	(2)(a), (b)
Sample Language	Appendix F
Sneak and Peek Warrants	(2)(b)(6)
Workplace Searches	
Generally	(1)(d)
Private Sector	(1)(d)(1)
Public Sector	(1)(d)(2)

Appendix C: H.R. 2459 Establishment of Department of Peace

<i>THIS SEARCH</i>	<i>THIS DOCUMENT</i>	<i>GO TO</i>
Next Hit	Forward	New Bills Search
Prev Hit	Back	HomePage
Hit List	Best Sections	Help
	Doc Contents	

H.R.2459

To establish a Department of Peace. (Introduced in the House)

TITLE I--ESTABLISHMENT OF DEPARTMENT OF PEACE

SEC. 101. ESTABLISHMENT OF DEPARTMENT OF PEACE.

(a) ESTABLISHMENT- There is hereby established a Department of Peace (hereinafter in this Act referred to as the 'Department'), which shall--

- (1) be a cabinet-level department in the executive branch of the Federal Government; and
- (2) be dedicated to peacemaking and the study of conditions that are conducive to both domestic and international peace.

(b) SECRETARY OF PEACE- There shall be at the head of the Department a Secretary of Peace (hereinafter in this Act referred to as the 'Secretary'), who shall be appointed by the President, with the advice and consent of the Senate.

(c) MISSION- The Department shall--

- (1) hold peace as an organizing principle, coordinating service to every level of American society;
- (2) endeavor to promote justice and democratic principles to expand human rights;
- (3) strengthen nonmilitary means of peacemaking;
- (4) promote the development of human potential;
- (5) work to create peace, prevent violence, divert from armed conflict, use field-tested programs, and develop new structures in nonviolent dispute resolution;
- (6) take a proactive, strategic approach in the development of policies that promote national and international conflict prevention, nonviolent intervention, mediation, peaceful resolution of conflict, and structured mediation of conflict;
- (7) address matters both domestic and international in scope; and
- (8) encourage the development of initiatives from local communities, religious groups, and nongovernmental organizations.

thereby inform and inspire national policy; and

(13) provide ethical-based and value-based analyses to the Department of Defense.

(c) INTERNATIONAL RESPONSIBILITIES- The Secretary shall--

(1) advise the Secretary of Defense and the Secretary of State on all matters relating to national security, including the protection of human rights and the prevention of, amelioration of, and de-escalation of unarmed and armed international conflict;

(2) provide for the training of all United States personnel who administer postconflict reconstruction and demobilization in war-torn societies;

(3) sponsor country and regional conflict prevention and dispute resolution initiatives, create special task forces, and draw on local, regional, and national expertise to develop plans and programs for addressing the root sources of conflict in troubled areas;

(4) provide for exchanges between the United States and other nations of individuals who endeavor to develop domestic and international peace-based initiatives;

(5) encourage the development of international sister city programs, pairing United States cities with cities around the globe for artistic, cultural, economic, educational, and faith-based exchanges;

(6) administer the training of civilian peacekeepers who participate in multinational nonviolent police forces and support civilian police who participate in peacekeeping;

(7) jointly with the Secretary of the Treasury, strengthen peace enforcement through hiring and training monitors and investigators to help with the enforcement of international arms embargoes;

(8) facilitate the development of peace summits at which parties to a conflict may gather under carefully prepared conditions to promote nonviolent communication and mutually beneficial solutions;

(9) submit to the President recommendations for reductions in weapons of mass destruction, and make annual reports to the President on the sale of arms from the United States to other nations, with analysis of the impact of such sales on the defense of the United States and how such sales affect peace;

(10) in consultation with the Secretary of State, develop strategies for sustainability and management of the distribution of international funds; and

(11) advise the United States Ambassador to the United Nations on matters pertaining to the United Nations Security Council.

(d) HUMAN SECURITY RESPONSIBILITIES- The Secretary shall address and offer nonviolent conflict resolution strategies to all relevant parties on issues of human security if such security is threatened by conflict, whether such conflict is geographic, religious, ethnic, racial, or class-based in its origin, derives from economic concerns (including trade or maldistribution of wealth), or is initiated through disputes concerning scarcity of natural resources (such as water and energy

(7) provide grants for peace studies departments in colleges and universities throughout the United States.

SEC. 103. PRINCIPAL OFFICERS.

(a) UNDER SECRETARY OF PEACE- There shall be in the Department an Under Secretary of Peace, who shall be appointed by the President, by and with the advice and consent of the Senate. During the absence or disability of the Secretary, or in the event of a vacancy in the office of the Secretary, the Under Secretary shall act as Secretary. The Secretary shall designate the order in which other officials of the Department shall act for and perform the functions of the Secretary during the absence or disability of both the Secretary and Under Secretary or in the event of vacancies in both of those offices.

(b) ADDITIONAL POSITIONS- (1) There shall be in the Department--

- (A) an Assistant Secretary for Peace Education and Training;
- (B) an Assistant Secretary for Domestic Peace Activities;
- (C) an Assistant Secretary for International Peace Activities;
- (D) an Assistant Secretary for Technology for Peace;
- (E) an Assistant Secretary for Arms Control and Disarmament;
- (F) an Assistant Secretary for Peaceful Coexistence and Nonviolent Conflict Resolution;
- (G) an Assistant Secretary for Human and Economic Rights; and
- (H) a General Counsel.

(2) Each of the Assistant Secretaries and the General Counsel shall be appointed by the President, by and with the advice and consent of the Senate.

(3) There shall be in the Department an Inspector General, who shall be appointed in accordance with the provisions in the Inspector General Act of 1978 (5 U.S.C. App.).

(4) There shall be in the Department four additional officers who shall be appointed by the President, by and with the advice and consent of the Senate. The officers appointed under this paragraph shall perform such functions as the Secretary shall prescribe, including--

- (A) congressional relations functions;
- (B) public information functions, including providing, through the use of the latest technologies, useful information about peace and the work of the Department;
- (C) management and budget functions; and
- (D) planning, evaluation, and policy development functions, including development of policies to promote the efficient and coordinated administration of the Department and its programs and encourage improvements in conflict resolution and violence prevention.

(a) IN GENERAL- There shall be in the Department an Office of International Peace Activities, the head of which shall be the Assistant Secretary for International Peace Activities. The Assistant Secretary for International Peace Activities shall carry out those functions in the Department affecting international peace activities and shall be a member of the National Security Council.

(b) RESPONSIBILITIES- The Assistant Secretary for International Peace Activities shall--

- (1) provide for the training and deployment of all Peace Academy graduates and other nonmilitary conflict prevention and peacemaking personnel;
- (2) sponsor country and regional conflict prevention and dispute resolution initiatives in countries experiencing social, political, or economic strife;
- (3) advocate the creation of a multinational nonviolent peace force;
- (4) provide training for the administration of postconflict reconstruction and demobilization in war-torn societies; and
- (5) provide for the exchanges between individuals of the United States and other nations who are endeavoring to develop domestic and international peace-based initiatives.

SEC. 107. OFFICE OF TECHNOLOGY FOR PEACE.

(a) IN GENERAL- There shall be in the Department an Office of Technology for Peace, the head of which shall be the Assistant Secretary of Technology for Peace. The Assistant Secretary of Technology for Peace shall carry out those functions in the Department affecting the awareness, study, and impact of developing new technologies on the creation and maintenance of domestic and international peace.

(b) GRANTS- The Assistant Secretary of Technology for Peace shall provide grants for the research and development of technologies in transportation, communications, and energy that--

- (1) are nonviolent in their application; and
- (2) encourage the conservation and sustainability of natural resources in order to prevent future conflicts regarding scarce resources.

SEC. 108. OFFICE OF ARMS CONTROL AND DISARMAMENT.

(a) IN GENERAL- There shall be in the Department an Office of Arms Control and Disarmament, the head of which shall be the Assistant Secretary of Arms Control and Disarmament. The Assistant Secretary of Arms Control and Disarmament shall carry out those functions in the Department affecting arms control programs and arms limitation agreements.

(b) RESPONSIBILITIES- The Assistant Secretary of Arms Control and Disarmament shall--

- (1) advise the Secretary on all interagency discussions and all international negotiations regarding the reduction and elimination of weapons of mass destruction throughout the world, including the dismantling of such weapons and the safe and secure storage of materials related thereto;
- (2) assist nations, international agencies and nongovernmental organizations in assessing

the head of which shall be the Assistant Secretary of Arms Control and Disarmament. The Assistant Secretary of Arms Control and Disarmament shall carry out those functions in the Department affecting arms control programs and arms limitation agreements.

(b) RESPONSIBILITIES- The Assistant Secretary of Arms Control and Disarmament shall--

- (1) advise the Secretary on all interagency discussions and all international negotiations regarding the reduction and elimination of weapons of mass destruction throughout the world, including the dismantling of such weapons and the safe and secure storage of materials related thereto;
- (2) assist nations, international agencies and nongovernmental organizations in assessing the locations of the buildup of nuclear arms;
- (3) develop nonviolent strategies to deter the testing or use of offensive or defensive nuclear weapons, whether based on land, air, sea, or in outer space;
- (4) serve as a depository for copies of all contracts, agreements, and treaties that deal with the reduction and elimination of nuclear weapons or the protection of outer space from militarization; and
- (5) provide technical support and legal assistance for the implementation of such agreements.

SEC. 109. OFFICE OF PEACEFUL COEXISTENCE AND NONVIOLENT CONFLICT RESOLUTION.

(a) IN GENERAL- There shall be in the Department an Office of Peaceful Coexistence and Nonviolent Conflict Resolution, the head of which shall be the Assistant Secretary for Peaceful Coexistence and Nonviolent Conflict Resolution. The Assistant Secretary for Peaceful Coexistence and Nonviolent Conflict Resolution shall carry out those functions in the Department affecting research and analysis relating to creating, initiating, and modeling approaches to peaceful coexistence and nonviolent conflict resolution.

(b) RESPONSIBILITIES- The Assistant Secretary for Peaceful Coexistence and Nonviolent Conflict Resolution shall--

- (1) study the impact of war, especially on the physical and mental condition of children (using the ten-point agenda in the United Nations Children's Fund report, State of the World's Children 1996, as a guide), which shall include the study of the effect of war on the environment and public health;
- (2) publish a monthly journal of the activities of the Department and encourage scholarly participation;
- (3) gather information on effective community peacebuilding activities and disseminate such information to local governments and nongovernmental organizations in the United States and abroad;
- (4) research the effect of violence in the media and make such reports available to the Congress annually; and

(5) sponsor conferences throughout the United States to create awareness of the work of the Department.

SEC. 110. OFFICE OF HUMAN RIGHTS AND ECONOMIC RIGHTS.

(a) IN GENERAL- There shall be in the Department an Office of Human Rights and Economic Rights, the head of which shall be the Assistant Secretary for Human Rights and Economic Rights. The Assistant Secretary for Human Rights and Economic Rights shall carry out those functions in the Department supporting the principles of the Universal Declaration of Human Rights passed by the General Assembly of the United Nations on December 10, 1948.

(b) RESPONSIBILITIES- The Assistant Secretary for Human Rights and Economic Rights shall--

(1) assist the Secretary, in cooperation with the Secretary of State, in furthering the incorporation of principles of human rights, as enunciated in the United Nations General Assembly Resolution 217A (III) of December 10, 1948, into all agreements between the United States and other nations to help reduce the causes of violence;

(2) gather information on and document human rights abuses, both domestically and internationally, and recommend to the Secretary nonviolent responses to correct abuses;

(3) make such findings available to other agencies in order to facilitate nonviolent conflict resolution;

(4) provide trained observers to work with nongovernmental organizations for purposes of creating a climate that is conducive to the respect for human rights;

(5) conduct economic analyses of the scarcity of human and natural resources as a source of conflict and make recommendations to the Secretary for nonviolent prevention of such scarcity, nonviolent intervention in case of such scarcity, and the development of programs of assistance for people experiencing such scarcity, whether due to armed conflict, maldistribution of resources, or natural causes; and

(6) assist the Secretary, in cooperation with the Secretary of State and the Secretary of the Treasury, in developing strategies regarding the sustainability and the management of the distribution of funds from international agencies, the conditions regarding the receipt of such funds, and the impact of those conditions on the peace and stability of the recipient nations.

SEC. 111. INTERGOVERNMENTAL ADVISORY COUNCIL ON PEACE.

(a) IN GENERAL- There shall be in the Department an advisory committee to be known as the Intergovernmental Advisory Council on Peace (hereinafter in this Act referred to as the 'Council'). The Council shall provide assistance and make recommendations to the Secretary and the President concerning intergovernmental policies relating to peace and nonviolent conflict resolution.

(b) RESPONSIBILITIES- The Council shall--

(1) provide a forum for representatives of Federal, State, and local governments to discuss peace issues;

(2) promote better intergovernmental relations; and

(3) submit, biennially or more frequently if determined necessary by the Council, a report to the Secretary, the President, and the Congress reviewing the impact of Federal peace activities on State and local governments.

SEC. 112. CONSULTATION REQUIRED.

(a) **CONSULTATION IN CASES OF CONFLICT-** (1) In any case in which a conflict between the United States and any other government or entity is imminent or occurring, the Secretary of Defense and the Secretary of State shall consult with the Secretary concerning nonviolent means of conflict resolution.

(2) In any case in which such a conflict is ongoing or recently concluded, the Secretary shall conduct independent studies of diplomatic initiatives undertaken by the United States and other parties to the conflict.

(3) In any case in which such a conflict has recently concluded, the Secretary shall assess the effectiveness of those initiatives in ending the conflict.

(4) The Secretary shall establish a formal process of consultation in a timely manner with the Secretary of the Department of State and the Secretary of the Department of Defense--

(A) prior to the initiation of any armed conflict between the United States and any other nation; and

(B) for any matter involving the use of Department of Defense personnel within the United States.

(b) **CONSULTATION IN DRAFTING TREATIES AND AGREEMENTS-** The executive branch shall consult with the Secretary in drafting treaties and peace agreements.

SEC. 113. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to carry out this Act at least 1 percent of the total amounts appropriated annually for the Department of Defense.

TITLE II--ADMINISTRATIVE PROVISIONS AND TRANSFERS OF AGENCY FUNCTIONS

SEC. 201. STAFF.

The Secretary may appoint and fix the compensation of such employees as may be necessary to carry out the functions of the Secretary and the Department. Except as otherwise provided by law, such employees shall be appointed in accordance with the civil service laws and their compensation fixed in accordance with title 5 of the United States Code.

SEC. 202. TRANSFERS.

There are hereby transferred to the Department the functions, assets, and personnel of--

(1) the Peace Corps;

(2) the United States Institute of Peace;

(3) the Office of the Under Secretary for Arms Control and International Security Affairs of the Department of State;

(4) the Gang Resistance Education and Training Program of the Bureau of Alcohol, Tobacco and Firearms; and

(5) the SafeFutures program of the Office of Juvenile Justice and Delinquency Prevention of the Department of Justice.

SEC. 203. CONFORMING AMENDMENTS.

Not later than 90 days after the date of the enactment of this Act, the Secretary shall prepare and submit to Congress proposed legislation containing any necessary and appropriate technical and conforming amendments to the laws of the United States to reflect and carry out the provisions of this Act.

TITLE III--FEDERAL INTERAGENCY COMMITTEE ON PEACE

SEC. 301. FEDERAL INTERAGENCY COMMITTEE ON PEACE.

There is established a Federal Interagency Committee on Peace (hereinafter in this Act referred to as the 'Committee'). The Committee shall--

(1) assist the Secretary in providing a mechanism to assure that the procedures and actions of the Department and other Federal agencies are fully coordinated; and

(2) study and make recommendations for assuring effective coordination of Federal programs, policies, and administrative practices affecting peace.

TITLE IV--ESTABLISHMENT OF PEACE DAY

SEC. 401. PEACE DAY.

All citizens should be encouraged to observe and celebrate the blessings of peace and endeavor to create peace on a Peace Day. Such day shall include discussions of the professional activities and the achievements in the lives of peacemakers.

<i>THIS SEARCH</i>	<i>THIS DOCUMENT</i>	<i>GO TO</i>
Next Hit	Forward	New Bills Search
Prev Hit	Back	HomePage
Hit List	Best Sections	Help
	Doc Contents	

Appendix D: Fact Sheet on Office of Homeland Security

ELECTRONIC PRIVACY INFORMATION CENTER

Office of Homeland Security Fact Sheet

Table of Contents:

[Date Established](#)

[Authority](#)

[Management](#)

[Budget](#)

[Actions Taken to Date](#)

[References](#)

DATE ESTABLISHED

September 20, 2001: President Bush announces the establishment of the Office of Homeland Security, and the appointment of Pennsylvania Governor Tom Ridge in his Address to a Joint Session of Congress and the American People.

"Today, dozens of federal departments and agencies, as well as state and local governments, have responsibilities affecting homeland security. These efforts must be coordinated at the highest level. So tonight I announce the creation of a Cabinet-level position reporting directly to me -- the Office of Homeland Security. And tonight I also announce a distinguished American to lead this effort, to strengthen American security: a military veteran, an effective governor, a true patriot, a trusted friend -- Pennsylvania's Tom Ridge. (Applause.) He will lead, oversee and coordinate a comprehensive national strategy to safeguard our country against terrorism, and respond to any attacks that may come."

October 8, 2001: President Bush issues Executive Order 13228 Establishing the Office of Homeland Security and the Homeland Security Council.

October 8, 2001: Tom Ridge sworn in as the first Director of the Office of Homeland Security.

March 21, 2002: Executive Order Establishing the President's Homeland Security Advisory Council and Senior Advisory Committees for Homeland Security.

AUTHORITY

- Executive Order 13228 Establishing the Office of Homeland Security and the Homeland Security Council enumerates the mission and functions of the Office of Homeland Security.
- A summary of the President's Executive Order.

The President's mission for the Office of Homeland Security is "to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks."

Section 3 of the President's Executive Order sets out in detail the functions of the

Office of Homeland Security, which shall be "to coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States."

In performing many of its functions, the Office is required to work with the Assistant to the President for National Security Affairs, and with other Federal, State, and local agencies, and private entities, as appropriate.

Section 3 provides that the Director of the Office of Homeland Security shall have the power to:

(b) develop and review a National Strategy on terrorism;

(c) coordinate information collection, analysis and sharing to detect threats of terrorism and activities of terrorists within the United States, and prioritize requirements for foreign intelligence collection. The Office shall:

- facilitate information collection by State and local government and private entities;
- "provide [foreign intelligence] requirements and priorities to the Director of Central Intelligence and other agencies";
- audit and ensure all executive departments' and agencies' technological capabilities to collect intelligence;
- "coordinate development of monitoring protocols and equipment for use in detecting the release of biological, chemical, and radiological hazards"; and
- ensure dissemination and exchange of intelligence and law enforcement information among the executive branch and, where appropriate, promote exchange of such information with and among state and local governments and private entities.

All executive departments and agencies are required to make available to OHS "all information relating to terrorist threats and activities within the United States."

(d) coordinate national efforts to prepare for and mitigate the consequences of terrorist threats or attacks within the United States, including:

- review all federal emergency response plans relating to terrorism within the United States;
- coordinate domestic exercises and simulations designed to assess and practice systems to respond to terrorism, and coordinate programs and activities for training federal, state, and local employees who would be called upon to respond to such a threat or attack;
- coordinate national efforts to ensure public health preparedness for a terrorist attack, including reviewing vaccination policies and reviewing the adequacy of and, if necessary, increasing vaccine and pharmaceutical stockpiles and hospital capacity;
- coordinate federal assistance to state and local authorities and NGOs to prepare for and respond to terrorism;
- implement review and evaluation programs and standards for national preparedness programs, including allocation of resources to implement changes based on such evaluations; and
- ensure the readiness and coordinated deployment of federal response teams to respond to terrorist threats or attacks.

(e) coordinate efforts to prevent terrorist attacks within the United States, including:

- facilitate the exchange of information among INS and customs agencies;
- ensure coordination among such agencies to prevent the entry of terrorists and terrorist materials and supplies into the United States and facilitate removal of such terrorists from the United States, when appropriate;
- coordinate efforts to investigate terrorist threats and attacks within the United States;
- coordinate efforts to improve the security of United States borders, territorial waters, and airspace in order to prevent acts of terrorism within the United States.

(f) coordinate efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks, including:

- strengthen measures for protecting energy production, transmission, and distribution services and critical facilities; other utilities; telecommunications; facilities that produce, use, store, or dispose of nuclear material; and other critical infrastructure services and critical facilities within the United States from terrorist attack;
- coordinate efforts to protect critical public and privately owned information systems within the United States from terrorist attack;
- develop criteria for reviewing whether appropriate security measures are in place at major public and privately owned facilities within the United States;
- coordinate domestic efforts to ensure that special events determined by appropriate senior officials to have national significance are protected from terrorist attack;
- coordinate efforts to protect transportation systems within the United States, including railways, highways, shipping, ports and waterways, and airports and civilian aircraft, from terrorist attack;
- coordinate efforts to protect United States livestock, agriculture, and systems for the provision of water and food for human use and consumption from terrorist attack; and
- coordinate efforts to prevent unauthorized access to, development of, and unlawful importation into the United States of, chemical, biological, radiological, nuclear, explosive, or other related materials that have the potential to be used in terrorist attacks.

(g) coordinate efforts to respond to and promote recovery from terrorist threats or attacks within the United States, including:

- coordinate efforts to ensure rapid restoration of transportation systems, energy production, transmission, and distribution systems; telecommunications; other utilities; and other critical infrastructure facilities after disruption by a terrorist threat or attack;
- coordinate efforts to ensure rapid restoration of public and private critical information systems after disruption by a terrorist threat or attack;
- work with the National Economic Council to coordinate efforts to stabilize United States financial markets after a terrorist threat or attack and manage the immediate economic and financial consequences of the incident;
- coordinate federal plans and programs to provide medical, financial, and other assistance to victims of terrorist attacks and their families; and
- coordinate containment and removal of any biological, chemical, radiological, explosive, or other hazardous materials, and coordinate efforts to mitigate the effects of such an attack.

(h) The Director of the OHS will be the individual primarily responsible for incident management:

- coordinating the domestic response efforts of all departments and agencies in

the event of an imminent terrorist threat and during and in the immediate aftermath of a terrorist attack within the United States;

- principal point of contact for and to the President with respect to coordination of such efforts.

(i) The Director of the OHS will review plans and preparations for ensuring the continuity of the Federal Government in the event of a terrorist attack that threatens the safety and security of the United States Government or its leadership.

(j) The Office, subject to the direction of the White House Office of Communications, shall:

- coordinate the strategy of the executive branch for communicating with the public in the event of a terrorist threat or attack within the United States;
- develop programs for educating the public about the nature of terrorist threats and appropriate precautions and responses.

(k) Legal analysis and legislative proposals. The Office will:

- coordinate a periodic review and assessment of the legal authorities available to executive departments and agencies to permit them to perform the functions described in this order;
- develop proposals for presidential action and legislative proposals for submission to the Office of Management and Budget to enhance the ability of executive departments and agencies to perform those functions.
- work with state and local governments to assess the adequacy of their legal authorities to permit them to detect, prepare for, prevent, protect against, and recover from terrorist threats and attacks.

(l) The Director, in conducting a budget review, will:

- identify programs that contribute to the Administration's strategy for homeland security;
- review and provide advice to the heads of departments and agencies for such programs;
- provide advice to the OMB on the level and use of funding in departments and agencies for homeland security-related activities;
- certify to the OMB the funding levels that the Director believes are necessary and appropriate for the homeland security-related activities of the executive branch.

- Executive Order Establishing the President's Homeland Security Advisory Council and Senior Advisory Committees for Homeland Security. (March 21, 2002)

This most recent order gives Director Ridge the authority to appoint the Executive Director of the President's Homeland Security Advisory Council (PHSAC) and the Chair and Vice Chair for each of the Senior Advisory Committees for Homeland Security (SACs). Director Ridge is authorized to convene meetings of the Council and Committee to provide advice to the President through Director Ridge (Section 2: Functions).

MANAGEMENT

Director of the Office of Homeland Security:

Biography of Governor Tom Ridge, Director of the Office of Homeland Security.

Other staff:

Deputy Director of the Office of Homeland Security: Admiral Steve Abbot.
 Deputy Assistant to the President for Homeland Security: Mark A. Holman.
 Deputy Assistant to the President for Legislative Affairs for the Office of Homeland Security: Becky Halkias.
 Special Assistant to the President and Executive Secretary for the Office of Homeland Security: Carl M. Buckholz.
 Special Assistant to the President and Public Liaison for the Office of Homeland Security: Barbara Chaffee.
 Special Assistant to the President and Director of Communications for Homeland Security: Susan Neely.
 Special Assistant to the President and Adviser for External Affairs on Homeland Security: Frank Cilluffo.
 Office of Homeland Security General Counsel: Ed McNally.
 Senior Director of Protection and Prevention: Major General Bruce Lawlor.
 Senior Director of Response and Recovery: Michael Byrne.
 Senior Director of Border Security: Brian Peterman.
 Senior Director of Policy and Plans: Richard Falkenrath.
Announcement of appointments and biographical information.

Total Staff:

- Approximately 80 staff.
- The Office was intended to have a staff of 100.

BUDGET

"Securing the Homeland, Strengthening the Nation," by President George W. Bush .

In this publication, the President outlines his vision for the operation of the Office of Homeland Security in more detail, including budgetary allocations and spending on specific programs.

Specifically, the report itemizes the spending under the President's four key budgetary goals that will be administered by the Office of Homeland Security, namely:

- Supporting First Responders
- Defending Against Bioterrorism
- Securing America's Borders
- Using 21st Century Technology to Secure the Homeland

Additional Budget Priorities administered under the Office of Homeland Security include:

- Transportation Security
- Federal Law Enforcement
- Citizen Corps
- Department of Defense and Intelligence Community
- Protecting our Critical Infrastructure

Director Ridge's National Strategy for Homeland Security "will encompass the full range of homeland security activities and will set priorities among them," thus directing the allocation of \$10.6 billion of the Federal Emergency Response Fund, as well as billions of dollars at the state and local levels. The FY2003 Federal Budget directs \$37.7 billion to homeland security.

The Budget for the Executive Office of the President, for Physical and IT Security in FY2002 was \$2 million, with an additional \$58 million in the 2002 Supplement when the Office of Homeland Security also came within this budgetary category. The FY2003 request for the Executive Office of the President Physical and IT Security and the Office of Homeland Security is \$48 million.

ACTIONS TAKEN TO DATE

(available at: <http://www.whitehouse.gov/homeland/archive.html>)

October 8, 2001: Governor Ridge Sworn-In to Lead Homeland Security, President Establishes Office of Homeland Security.

October 18, 2001: Director Ridge, Leaders Discuss Homeland Security and Anthrax.

October 19, 2001: Director Ridge Briefs Media at Week's End on Homeland Security Issues and Anthrax.

October 22, 2001: Director Ridge Discusses Anthrax Situation

October 25, 2001: Gov. Ridge, Medical Authorities Discuss Anthrax

October 29, 2001: Ridge, Thompson Hold Briefing

October 30, 2001: Tuesday's Homeland Security Briefing: "one of the great challenges I have as the Director of Homeland Security, in giving you timely and accurate and complete information with regard to this threat assessment and the threat alert."

November 7, 2001: Wednesday's Homeland Security Briefing. Reflecting on some of the activity of the Homeland Security Office, Governor Ridge reported meetings with, among others, members of Congress, a business roundtable, Governors and Mayors, NASCAR, the British Ambassador.

November 28, 2001: Governor Ridge Speaks at Homeland Security and Defense Conference (selected quotes):

"Now, the Defense Department takes a long-range approach to its budget needs, Homeland Security will do likewise with a multiyear budget plan, a plan that cuts across all agencies, a plan that not only addresses present urgent needs as we build a foundation for national homeland strategy, for security strategy, but also works to get ahead of the threat. In other words, we're not preparing to fight the wars of the past, we're creating a blueprint to win the wars of the future."

"I think one of the challenges that the Office of Homeland Security has is to make sure that it becomes a permanent part of how the federal government does business... But I think our long-term best interests will be served if we create

structures and relationships that just become a permanent part of how we do business and how the government provides service and security for the long-term.

"One of the more interesting ideas I received, it was generated from a conversation I had with the airline industry, happened to involve the voluntary deployment of biometric cards. Now, I know there are some people that favor face recognition technology. I happen to believe that whatever the technology that can be applied with the greatest impact immediately because this technology is going to change, we will deploy the best first; and as it changes, let's change our system. Let's try to be as flexible and as quick to respond in government, as agencies and organizations and companies and individuals are outside of government. So I'll let the experts decide what is the best technology to be deployed."

December 3, 2001: Governor Ridge Holds Homeland Security Briefing and Issues an Alert, "discerning specific, credible information and concluding that it gives rise to a reminder to America that we're still at war."

December 12, 2001: Governor Ridge and John Manley, then Canada's Minister of Foreign Affairs, sign the "Smart Border Declaration" with a 30-point action plan that will help speed and secure the flow of people and goods between the United States and Canada.

January 23, 2002: Governor Ridge Addresses U.S. Conference of Mayors: "One of the opportunities the President has given this office, and I think it's an opportunity that this country should embrace, as we take a look at ourselves through the lens of security, we may find that if we look a little bit beyond just security, we'll find ways to dramatically improve our communities, our states and our country, as well."

January 24, 2002: President Announces Substantial Increases in Homeland Security Budget: "Thirty-eight billion dollars is the total request. Double over 2002. It's the beginning of a homeland defense initiative which is going to last throughout my administration."

February 24, 2002: Homeland Security Director Speaks at the National Governor's Associations Winter Meeting in Washington:

"In the President's executive order, he specifically directed this office to design and implement a national strategy, not a federal one. And by implication, that means that the federal government, working with the state government, working with local governments. We need to find a way to be as seamless as we possibly can."

"But the President has said, take a look at the borders with our friends in the north in Canada, and in the south in Mexico, and come up with some smart border agreements -- not dealing just with security, but dealing with the enhancement of commerce, dealing with drug interdiction, dealing with immigration."

"I know that John [Magaw] has said, no more special treatment for frequent fliers. But I do think that this might be a great opportunity for us to do some work with biometrics, and get a trusted flier program."

February 25, 2002: President Bush Meets with Nation's Governors. Regarding the appointment of Governor Ridge to the Office of Homeland Security: "And I said, would you come and be a member of my Cabinet, be sitting at my right hand there, and design a national strategy for homeland security? And, fortunately, for the country, he said yes."

March 4, 2002: Gov Ridge Speaks at U.S. Embassy in Mexico regarding Border Security initiatives

March 8, 2002: Governor Ridge Discusses Smart Border Plan with the Deputy P.M. of Canada. Proposes expanding ID card program for pre-screened travelers.

March 12, 2002: Governor Ridge Announces New Homeland Security Advisory System: "Now, the decision to name a threat condition will rest with the Attorney General, after consulting with members of the Homeland Security Council, after consulting with me. We're asking all federal departments and agencies make this system work immediately, integrate their plans into this advisory system, and work with us over the next 135 days to a final system."

REFERENCES

- [OHS web site.](#)
- [Executive Order Establishing Office of Homeland Security.](#)
- [President George W. Bush: "Securing the Homeland, Strengthening the Nation."](#)
- [Biography of Governor Tom Ridge, Director of the Office of Homeland Security.](#)
- [Announcement of staff appointments and biographical information.](#)
- [Executive Order Establishing the President's Homeland Security Advisory Council and Senior Advisory Committees for Homeland Security.](#)

[EPIC Homeland Security Page](#) | [EPIC Open Government Page](#) | [EPIC Home Page](#)

Appendix E: Echelon Code Words

Rewson, SAFE, Waihopai, INFOSEC, ASPIC, MI6, Information Security, SAI, Information Warfare, IW, IS, Privacy, Information Terrorism, Terrorism Defensive Information, Defense Information Warfare, Offensive Information, Offensive Information Warfare, The Artful Dodger, NAlA, SAPM, ASU, ASTS, National Information Infrastructure, InfoSec, SAO, Reno, Compsec, JICS, Computer Terrorism, Firewalls, Secure Internet Connections, RSP, ISS, JDF, Ermes, Passwords, NAAP, DefCon V, RSO, Hackers, Encryption, ASWS, CUN, CISU, CUSI, M.A.R.E., MARE, UFO, IFO, Pacini, Angela, Espionage, USDOJ, NSA, CIA, S/Key, SSL, FBI, Secert Service, USSS, Defcon, Military, White House, Undercover, NCCS, Mayfly, PGP, SALDV, PEM, resta, RSA, Perl-RSA, MSNBC, bet, AOL, AOL TOS, CIS, CBOT, AIMSX, STARLAN, 3B2, BITNET, SAMU, COSMOS, DATTA, Furbys, E911, FCIC, HTCIA, IACIS, UT/RUS, JANET, ram, JICC, ReMOB, LBETAC, UTU, VNET, BRLO, SADCC, NSLEP, Daffy Duck, SAACLANTCEN, FALN, 877, NAVELEXSYSSECENGCEN, BZ, CANSLO, CBNRC, CIDA, JAVA, rsta, Active X, Compsec 97, RENS, LLC, DERA, JIC, rip, rb, Wu, RDI, Mavricks, BIOL, Meta-hackers, ^?, SADT, Steve Case, Tools, RECCEX, Telex, Aldergrove, OTAN, monarchist, NMIC, NIOG, IDB, MID/KL, NADIS, NMI, SEIDM, BNC, CNCIS, STEEPLEBUSH, RG, BSS, DDIS, mixmaster, BCCI, BRGE, Europol, SARL, Military Intelligence, JICA, Scully, recondo, Flame, Infowar, FRU, Bubba, Freeh, Archives, ISADC, CISSP, Sundevil, jack, Investigation, JOTS, ISACA, NCSA, ASVC, spook words, RRF, 1071, Bugs Bunny, Verisign, Secure, ASIO, Lebed, ICE, NRO, Lexis-Nexis, NSCT, SCIF, FLiR, JIC, bce, Lacrosse, Flashbangs, HRT, IRA, EODG, DIA, USCOI, CID, BOP, FINCEN, FLETC, NIJ, ACC, AFSPC, BMDO, site, SASSTIXS, NAVWAN, NRL, RL, NAVWCWPNS, NSWC, USAFA, AHPCRC, ARPA, SARD, LABLINK, USACIL, SAPT, USCG, NRC, ~, O, NSA/CSS, CDC, DOE, SAAM, FMS, HPC, NTIS, SEL, USCODE, CISE, SIRC, CIM, ISN, DJC, LLNL, bemd, SGC, UNCPCJ, CFC, SABENA, DREO, CDA, SADR, DRA, SHAPE, bird dog, SAACLANT, BECCA, DCJFTF, HALO, SC, TA SAS, Lander, GSM, T Branch, AST, SAMCOMM, HAHO, FKS, 868, GCHQ, DITSA, SORT, AMEMB, NSG, HIC, EDI, benelux, SAS, SBS, SAW, UDT, EODC, GOE, DOE, SAMF, GEO, JRB, 3P-HV, Masuda, Forte, AT, GIGN, Exon Shell, radint, MB, CQB, TECS, CONUS, CTU, RCMP, GRU, SASR, GSG-9, 22nd SAS, GEOS, EADA, SART, BBE, STEP, Echelon, Dictionary, MD2, MD4, MDA, diwn, 747, ASIC, 777, RDI, 767, MI5, 737, MI6, 757, Kh-11, EODN, SHS, ^X, Shayet-13, SADMS, Spetznaz, Recce, 707, CIO, NOCS, Halcon, NSS, Duress, RAID, Uziel, wojo, Psyops, SASCOM, grom, NSIRL, D-11, DF, ZARK, SERT, VIP, ARC, S.E.T. Team, NSWG, MP5k, SATKA, DREC, DEVGRP, DSD, FDM, GRU, LRTS, SIGDEV, NACSI, MEU/SOC, PSAC, PTT, RFI, ZL31, SIGDASYS, TDM. SUKLO, Schengen, SUSLO, TELINT, fake, TEXTA. ELF, LF, MF, Mafia, JASSM, CALCM, TLAM, Wipeout, GH, SIW, MEII, C2W, Burns, Tomlinson, Ufologico Nazionale, Centro, CICAP, MIR, Belknap, Tac, rebels, BLU-97 A/B, 007, nowhere.ch, bronze, Rubin, Arnett, BLU, SIGS, VHF, Recon, peapod, PA598D28, Spall, dort, 50MZ, 11Emc Choe, SATCOMA, UHF, The Hague, SHF, ASIO, SASP, WANK, Colonel, domestic disruption, 5ESS, smuggle, Z-200, 15kg, DUVDEVAN, RFX, nitrate, OIR, Pretoria, M-14, enigma, Bletchley Park, Clandestine, NSO, nkvd, argus, afsatcom, CQB, NVD, Counter Terrorism Security, Enemy of the State, SARA, Rapid Reaction, JSOFC3IP, Corporate Security, OSAll, 192.47.242.7, Baldwin,

Wilma, ie.org, cospo.osis.gov, Police, Dateline, Tyrell, KMI, lee, Pod, 9705 Samford Road, 20755-6000, sniper, PPS, ASIS, ASLET, TSCM, Security Consulting, M-x spook, Z-150T, Steak Knife, High Security, Security Evaluation, Electronic Surveillance, MI-17, ISR, NSAS, Counterterrorism, real, spies, IWO, eavesdropping, debugging, CCSS, interception, COCOT, NACSI, rhost, rhosts, ASO, SETA, Amherst, Broadside, Capricorn, NAVCM, Gamma, Gorizont, Guppy, NSS, rita, ISSO, submiss, ASDIC, .tc, 2EME REP, FID, 7NL SBS, tekka, captain, 226, .45, nonac, .li, Tony Poe, MJ-12, JASON, Society, Hmong, Majic, evil, zipgun, tax, bootleg, warez, TRV, ERV, rednoise, mindwar, nailbomb, VLF, ULF, Paperclip, Chatter, MKULTRA, MKDELTA, Bluebird, MKNAOMI, White Yankee, MKSEARCH, 355 ML, Adriatic, Goldman, Ionosphere, Mole, Keyhole, NABS, Kilderkin, Artichoke, Badger, Emerson, Tzvrif, SDIS, T2S2, STTC, DNR, NADDIS, NFLIS, CFD, BLU-114/B, quarter, Cornflower, Daisy, Egret, Iris, JSOTF, Hollyhock, Jasmine, Juile, Vinnell, B.D.M., Sphinx, Stephanie, Reflection, Spoke, Talent, Trump, FX, FXR, IMF, POCSAG, rusers, Covert Video, Intiso, r00t, lock picking, Beyond Hope, LASINT, csystems, .tm, passwd, 2600 Magazine, JUWTF, Competitor, EO, Chan, Pathfinders, SEAL Team 3, JTF, Nash, ISSAA, B61-11, floss, Alouette, executive, Event Security, Mace, Cap-Stun, stakeout, ninja, ASIS, ISA, EOD, Oscor, Tarawa, COSMOS-2224, COSTIND, hit word, hitword, Hitwords, Regli, VBS, Leuken-Baden, number key, Zimmerwald, DDPS, GRS, AGT. AMME, ANDVT, Type I, Type II, VFCT, VGPL, WHCA, WSA, WSP, WWABNCP, ZNI1, FSK, FTS2000, GOSIP, GOTS, SACS STU-III, PRF, PMSP, PCMT, I&A, JRSC, ITSDN, Keyer, KG-84C, KWT-46, KWR-46, KY-75, KYV-5, LHR, PARKHILL, LDMX, LEASAT, SNS, SVN, TACSAT, TRANSEC, DONCAF, EAM, DSCS, DSNET1, DSNET2, DSNET3, ECCM, EIP, EKMS, EKMC, DDN, DDP, Merlin, NTT, SL-1, Rolm, TIE, Tie-fighter, PBX, SLI, NTT, MSCJ, MIT, 69, RIT, Time, MSEE, Cable & Wireless, CSE, SUW, J2, Embassy, ETA, Porno, Fax, finks, Fax encryption, white noise, Fernspah, MYK, GAFE, forecast, import, rain, tiger, buzzer, N9, pink noise, CRA, M.P.R.I., top secret, Mossberg, 50BMG, Macintosh Security, freedom, Macintosh Internet Security, OC3, Macintosh Firewalls, Unix Security, VIP Protection, SIG, sweep, Medco, TRD, TDR, Z, WTO, sweeping, SURSAT, 5926, TELINT, Audiotel, Harvard, 1080H, SWS, Asset, Satellite imagery, force, NAIAG, Cypherpunks, NARF, 127, Coderpunks, TRW, remailers, replay, redheads, RX-7, explicit, FLAME, J-6, Pornstars, AVN, Playboy, ISSSP, Anonymous, W, Sex, chaining, codes, Nuclear, 20, subversives, SLIP, toad, fish, data havens, unix, c, a, b, d, SUBACS, the, Elvis, quiche, DES, 1*, N-ISDN, NLSP, OTAR, OTAT, OTCIXS, MISSI, MOSAIC, NAVCOMPARS, NCTS, NESP, MILSATCOM, AUTODIN, BLACKER, C3I, C4I, CMS, CMW, CP, SBU, SCCN, SITOR, SHF/DOD, Finksburg MD, Link 16, LATA, NATIA, NATOA, sneakers, UXO, (), OC-12, counterintelligence, Shaldag, sport, NASA, TWA, DT, gtegs, nowhere, .ch, hope, emc, industrial espionage, SUPIR, PI, TSCI, spookwords, industrial intelligence, H.N.P., SUAEWICS, Juiliett Class Submarine, Locks, qrss, loch, 64 Vauxhall Cross, Ingram Mac-10, wwics, sigvoice, ssa, E.O.D., Vx, SEMTEX, penrep, racial, OTP, OSS, Siemens, RPC, Met, CIA-DST, INI, watchers, keebler, contacts, Blowpipe, BTM, CCS, GSA, Kilo Class, squib, primacord, RSP, Z7, Becker, Nerd, fangs, Austin, nojd, Comirex, GPMG, Speakeasy, humint, GEODSS, SORO, M5, BROMURE, ANC, zone, SBI, DSS, S.A.I.C., Minox, Keyhole, SAR, Rand

Corporation, Starr, Wackenhutt, EO, burhop, Wackendude, mol, Shelton, 2E781, F-22, 2010, JCET, cocaine, Vale, IG, Kosovo, Dake, 36,800, GBC, Hillal, Pesec, Hindawi, GGL, NAICC, CTU, botux, Virii, CCC, ISPE, CCSC, Scud, SecDef, Magdeyev, VOA, Kosiura, Small Pox, Tajik, +=, Blacklisted 411, TRDL, Internet Underground, BX, XS4ALL, wetsu, muezzin, Retinal Fetish, WIR, Fetish, FCA, Yobie, forschung, emm, ANZUS, Reprieve, NZC-332, edition, cards, mania, 701, CTP, CATO, Phon-e, Chicago Posse, NSDM, 10ck, beanpole, spook, keywords, QRR, PLA, TDYC, W3, CUD, CdC, Weekly World News, Zen, World Domination, Dead, GRU, M72750, Salsa, 7, Blowfish, Gorelick, Glock, Ft. Meade, NSWT, press-release, WISDIM, burned, Indigo, wire transfer, e-cash, Bubba the Love Sponge, Enforcers, e-gold, Digicash, zip, SWAT, Ortega, PPP, NACSE, crypto-anarchy, ^X, AT&T, SGI, SUN, MCI, Blacknet, ISM, JCE, Middleman, KLM, Blackbird, NSV, GQ360, X400, Texas, jihad, SDI, BRIGAND, Uzi, Fort Meade, *&, gchq.gov.uk, supercomputer, bullion, 3, NTTC, Blackmednet, :, Propaganda, ABC, Satellite phones, IWIS, PDD, Planet-1, ISTA, rs9512c, Jiang Zemin, South Africa, Sergeyeve, Montenegro, Toeffler, Rebollo, sorot, Yucca Mountain, FARC, Toth, Xu Yongyue, Bach, Razor, AC, cryptanalysis, nuclear, 52 52 N - 03 03 W, Morgan, Canine, GEBA, INSCOM, MEMEX, Stanley, FBI, Panama, fissionable, Sears Tower, NORAD, Delta Force, SEAL, virtual, WASS, WID, Dolch, secure shell, screws, Black-Ops, O/S, Area51, SABC, basement, ISWG, \$@, data-haven, NSDD, black-bag, rack, TEMPEST, Goodwin, rebels, ID, MD5, IDEA, garbage, market, beef, Stego, ISAF, unclassified, Sayeret Tzanhanim, PARASAR, Gripan, pigr, curly, Taiwan, guest, utopia, NSG, orthodox, CCSQ, Alica, SHA, Global, gorilla, Bob, UNSCOM, Fukuyama, Manfurov, Kvashnin, Marx, Abdurahmon, snullen, Pseudonyms, MITM, NARF, Gray Data, VLSI, mega, Leitrim, Yakima, NSES, Sugar Grove, WAS, Cowboy, Gist, 8182, Gatt, Platform, 1911, Geraldton, UKUSA, veggie, XM, Parvus, NAVSVS, 3848, Morwenstow, Consul, Oratory, Pine Gap, Menwith, Mantis, DSD, BVD, 1984, blow out, BUDS, WQC, Flintlock, PABX, Electron, Chicago Crust, e95, DDR&E, 3M, KEDO, iButton, R1, erco, Toffler, FAS, RHL, K3, Visa/BCC, SNT, Ceridian, STE, condor, CipherTAC-2000, Etacs, Shipiro, ssor, piz, fritz, KY, 32, Edens, Kiwis, Kamumaruha, DODIG, Firefly, HRM, Albright, .SC, Bellcore, rail, csim, NMS, 2c, FIPS140-1, CAVE, E-Bomb, CDMA, Fortezza, 355ml, ISSC, cybercash, NAWAS, government, NSY, hate, speedbump, joe, illuminati, BOSS, Kourou, Misawa, Morse, HF, xechelon.org, P415, ladylove, filofax, Gulf, lamma, Unit 5707, Sayeret Mat'Kal, Unit 669, Sayeret Golani, Lanceros, Summercon, NSADS, president, ISFR, freedom, ISSO, walburn, Defcon VI, DC6, Larson, P99, c4i.org, HERF pipe-bomb, 2.3 Oz., cocaine, \$, imapct, Roswell, ESN, COS, E.T., credit card, b9, fraud, ST1, assassinate, virus, ISCS, ISPR, .VA, anarchy, rogue, mailbomb, 888, Chelsea, 1997, Whitewater, MOD, York, plutonium, William Gates, clone, BATF, SGDN, Nike, WWSV, Atlas, IWWSVCS, Delta, TWA, Kiwi, PGP 2.6.2., PGP 5.0i, PGP 5.1, siliconpimp, SASSTIXS, IWG, Lynch, 414, Face, Pixar, IRIDF, NSRB, eternity server, Skytel, Yukon, Templeton, Johohonbu, LUK, Jackson, Cohiba, Soros, Standford, niche, ISEP, ISEC, 51, H&K, USP, ^, sardine, bank, EUB, USP, PCS, NRO, Red Cell, NSOF, DC7, Glock 26, snuffle, Patel, package, ISI, INR, INS, GRU, RUOP, GSS, NSP, SRI, Ronco, Armani, BOSS, Chobetsu, FBIS, BND, SISDE, FSB, BfV, IB, froglegs, JITEM, SADF, advise, TUSA, LITE, PKK, HoHoCon, SISMI, ISG, FIS, MSW, Spyderco, UOP, SSCI,

NIMA, HAMASMOIS, SVR, SIN, advisors, SAP, Monica, OAU, PFS, Aladdin, AG, chameleon man, Hutsul, CESID, Bess, rail gun, .375, Peering, CSC, Tangimoana Beach, Commecen, Vanuatu, Kwajalein, LHI, DRM, GSGI, DST, MITI, JERTO, SDF, Koancho, Blenheim, Rivera, Kyudanki, varon, 310, 17, 312, NB, CBM, CTP, Sardine, SBIRS, jaws, SGDN, ADIU, DEADBEEF, IDP, IDF, Halibut, SONANGOL, Flu, &, Loin, PGP 5.53, meta, Faber, SFPD, EG&G, ISEP, blackjack, Fox, Aum, AIEWS, AMW, RHL, Baranyi, WORM, MP5K-SD, 1071, WINGS, cdi, VIA, DynCorp, UXO, Ti, WWSP, WID, osco, Mary, honor, Templar, THAAD, package, CISD, ISG, BIOLWPN, JRA, ISB, ISDS, chosen, LBSD, van, schloss, secops, DCSS, DPSD, LIF, J-Star, PRIME, SURVIAC, telex, Analyzer, solo, embassy, Golf, B61-7, Maple, Tokyo, ERR, SBU, Threat, JPL, Tess, SE, Alex, EPL, SPINTCOM, FOUO, ISS-ADP, Merv, Mexico, SUR, Gorel, blocks, SO13, Rojdykarna, RSOC, USS Banner, S511, 20755, ytcraacker, airframe, ज्या.com, Furby, PECSENC, football, Agfa, 3210, Crowell, moore, 510, OADR, Smith, toffee, FIS, N5P6, isn@c4i.org, EuroFed, SP4, Walnut, shelter, Crypto AG