INTERNET POLICY INSTITUTE

BRIEFING THE PRESIDENT

What the Next President of the United States Needs to Know About the Internet and Its Transformative Impact on Society

THE INTERNET, LAW ENFORCEMENT AND SECURITY

by Scott Charney
Principal, PricewaterhouseCoopers

PRICEWATERHOUSECOOPERS

BRIEFING THE PRESIDENT

What the Next President of the United States Needs to Know About the Internet and Its Transformative Impact on Society

More than a dozen leaders of the information revolution are contributing to a compilation of open letters to the next President of the United States titled *Briefing The President: What the Next President of the United States Needs to Know About the Internet and Its Transformative Impact on Society*. IPI's *Briefing The President* project aims to educate the new President and other elected officials about the fundamental nature of the Internet and the most important policy issues that will affect its future in the coming years.

The papers are distributed monthly, beginning last year in November, and continuing through the presidential election in November 2000, and are posted on IPI's web site. At the end of this year, the 13 papers will be published in book form and presented to the President-elect. The papers are written by experts whose experience in government, the sciences, academia, and private industry give them unique insight; some of the authors include former Federal Reserve Vice Chairman Alice Rivlin, AT&T CEO Michael Armstrong, WorldCom Senior Vice President Vinton G. Cerf, Corporation for National Research Initiatives Chairman Robert E. Kahn, and Covad Communications CEO Robert Knowling Jr. The Internet Policy Institute offers the opportunity to write Response papers to the published *Briefing The President* papers.

IPI INTERNET POLICY INSTITUTE

PRICEWATERHOUSECOOPERS

THE INTERNET, LAW ENFORCEMENT AND SECURITY

by Scott Charney,
Principal, PricewaterhouseCoopers

INTRODUCTION

We are in our fourth revolution. We were hunters and gatherers; then agrarian; next industrial; and now digital. With each major revolution, society has embraced change for its obvious benefits, paying scant attention to the predicable harms that would follow. For example, the Industrial Age promised greater production and efficiency, lower cost goods and a dramatic increase in our standard of living. Only after the Industrial Age was unleashed did society begin to focus on the other results: acid rain, sweatshops, and child labor, just to name a few.

The digital revolution has proved to be no different. The growth of the Internet has, for the most part, been fueled by its huge potential, both real and imagined. E-commerce figures prove that the Internet is bringing astounding commercial growth, with only greater rewards to follow.[1] The changes for individuals have been no less dramatic, with an ever-greater ability to engage in political discourse, find the most obscure information, and communicate with friends, family, and colleagues around the world.

But like past revolutions, this one too has its darker side. Since the value of information lies in its use, the Information Age has stirred debate over the collection and use of information and the seemingly unstoppable erosion of privacy.[2] As a communications medium, the Internet allows any individual to publish globally, without the fact-checking and editorial controls normally present in traditional large-scale media outlets.

Although this certainly has benefits, the fact remains that some speech crosses the line between proper and unfair (e.g., defamation), and the potential for causing damage increases with the size of the audience. And, of course, there is computer crime, a term often meant to include both hacking (computer abuse affecting the confidentiality, integrity or availability of data) and the use of computers to facilitate traditional offenses (e.g., Internet fraud and the distribution of child pornography). Significantly, in both civil and criminal cases, the Internet's attributes of global connectivity and lack of traceability may allow speech or action without accountability, no matter how harmful the consequences.

In response to criminal activity—including military and economic espionage—law enforcement and national security personnel have struggled to remain effective in an increasingly complex technological world. Their efforts have not been without controversy. From Clipper to Carnivore, they have been under attack from all sides: markets, civil libertarians, Congress, and the media.

As is so often the case in such passionate debates, the problem is not just the merits (which each side can claim in abundance), but also the process. Simply put, the problems posed by this revolution are too complex to be addressed as they are being done today: ad hoc and reactively. Instead, we should reassess certain fundamental assumptions about how to protect public safety and national security. Even more expansively, we should undertake a comprehensive review of the way in which we, as a society, balance the needs of commerce, law enforcement, national security, and privacy.

THE SECURITY DILEMMA

The Internet was designed as a military communications network. As such, its early users were military personnel, government defense contractors, and certain academic institutions. Simply put, in the beginning the Internet was available only to a group of trusted users, Internet crime was not a concern, and security was not critical. In the early 1980?s, however, IBM came out with the personal computer and the government declared the Internet a public resource. Suddenly, everyone was able to access the Internet, and the Internet lacked security.

As the hacker attacks began, the scope of the insecurity problem became clearer. Computer networks not only had a large number of known vulnerabilities, but new vulnerabilities were being reported weekly. Studies began to confirm the scope of the problem. For example, a Computer Security Institute Survey in 1995 reported that losses from FBI-reported computer crime had already reached $2 billion dollars.[3] Another survey revealed that 98.5% of the 182 respondents indicated that their businesses had been victims of a computer-related crime, with 43.3% saying that they had been victims more than twenty-five times.[4] But even these surveys were viewed as only the tip of the iceberg; virtually all computer crime

experts reasoned that most computer crimes were either not detected or, if they were, not reported.

This supposition was confirmed by a controlled study in which the United States Department of Defense attacked its own machines. Of the 38,000 machines attacked, 24,700 (65%) were penetrated. Only 988 (4%) of the penetrated sites realized they were compromised, and only 267 (27%) of those sites reported the attack. This in an agency with mandatory reporting and a staff that recognizes the importance of following orders. Moreover, to the extent the military has long been required to protect state and military secrets, it is more security conscious than most civilian agencies and private companies.

These broad studies have been supplemented by specific cases raising concrete concerns. Hackers have attacked the confidentiality of data, stealing Defense Department information and medical data.[5] Data integrity has also been affected, sometimes noticeably (a defaced Web page), sometimes in ways meant not to be detected and therefore more dangerous (e.g., an individual hacked a courthouse, apparently in an attempt to commute his prison sentence to probation). Finally, there have been serious denial of service attacks, such as the "Morris worm," which shut down thousands of computers as far back as 1988, and the more recent distributed denial of service attacks affecting key institutions such as Yahoo and CNN.

These studies and cases have led to more advanced thinking about the risks created by our increasing dependence on information technology. With society becoming ever more dependent on computers, it is now recognized that the disruption of our networks could seriously affect national security, public safety and economic prosperity. The disruption of power delivery, transportation services, banking and finance systems, and telecommunications systems could seriously disrupt the everyday lives of our citizens. Of greater concern is the potential for a cascading effect: how will attacks on one network lead to the failure of others? For example, if the telecommunications infrastructure is disabled, how will the banking and finance infrastructure, which relies upon telecommunications for electronic funds transfers, be affected?

The concern is not hypothetical: there has already been a "cascading effect" case. In the town of Worcester, Massachusetts, a juvenile attacked a telephone switch. In the course of the hack, the computer asked "Do you wish to reset the switch? (Y/N)." The hacker entered "Y", thus eliminating all of the custom settings of the switch and disabling phone service in the local area. A hacked phone switch, lost phone service.

But that was not all, for this switch also serviced a local airport. The tower was unmanned, and as planes approached to land they would radio the tower, which would automatically send a signal—across the telecommunications network—to activate the landing lights on the runway. As the next plane arrived, the radio signal was sent, but the disabled telephone switch prevented the landing lights from activating, and the airport had to be closed. Attack on a telecommunications network; failure of a transportation system. In this case, it was a juvenile and a small airport. What happens when terrorists attack the phone switches responsible for O'Hare?

THE PUBLIC SAFETY/ NATIONAL SECURITY CONUNDRUM

After years of debate over encryption policy, a press conference was held to announce that the United States Government was substantially relaxing export controls on encryption products.[6] At the press conference, then-Deputy Secretary of Defense John Hamre made a critically important statement that was not reported by those members of the press in attendance. He said, "law enforcement is now responsible for home defense." Indeed, the world had changed.

Throughout our history, citizens have relied upon government to protect public safety and national security. But all threats are not the same, and we have created different organizations and mechanisms for addressing different threats. To protect citizens against crime, we hire, train and equip law enforcement personnel. To protect us against those who would steal our military secrets or attack our vital state interests, we rely upon the intelligence community, both affirmatively to collect foreign intelligence, and defensively through counterintelligence techniques. Counterintelligence techniques are also used to protect economic secrets from foreign threats.[7] Finally, to address the military threat posed by another state, we fund a military, supporting personnel, equipment and weapons. In short, depending upon the threat, we deploy a different resource, and each resource plays by its own set of rules.[8]

This traditional model works, however, only when one can identify the nature of the attack; specifically, who is attacking and for what reason. This traditional model fails in the Information Age because when computers are under attack, the "who" and "why" are unknown. By way of example, many years ago a Russian military plane shot down a Korean civilian jetliner. For a long time, notwithstanding Russian claims of non-responsibility, it was widely believed that state action, or at least rogue military action, was responsible. Why? Because civilians do not have access to fighter jets.

But the notion that only states have access to weapons of war is no longer correct, at least not if information warfare is considered. Simply put, we have distributed a technology that is far more powerful than most that are placed in the public domain. Traditional vigilance regarding states that support terrorism, political unrest,

or are otherwise considered "rogue" (i.e., "nations of concern") are now supplemented by threats from "individuals of concern," a far larger pool, and one that is harder to identify and police.[9] As a result, an attack upon the Defense Department may come not only from a foreign nation conducting information warfare, but also from juveniles on the West Coast, as it did in Solar Sunrise (the case name for a widespread attack against the U.S. Department of Defense).[10] To the extent the country detects a cyberattack but does not know who is attacking (a juvenile, a criminal, a spy, or a nation-state bent on committing information warfare), what resources should it deploy in response?

The most likely answer—at least pursuant to current thinking—is law enforcement. This is because, with few exceptions, any attack on United States' computers will violate the Computer Fraud and Abuse Act, regardless of the identity and motive of the attacker.[11] Thus, Secretary Hamre's comment about home defense. But does this "default setting" make sense, and what will be the end result if law enforcement spends months investigating a "cybercrime" only to find another country is engaging in espionage or, worse, information warfare?[12] By analogy, it would be like sending the FBI to Hawaii on December 7, 1941 to investigate a trespass by Japan. Of course, the example is absurd because in the physical world, the differences between crime, espionage, and war are often self-evident. In the cyberworld this is not so, and we must rethink how to protect ourselves from attacks even when critical decisional information is lacking.

THE EVOLVING ROLE OF MARKETS

It would be difficult enough if this were the sole challenge facing society, but we must also reevaluate the interplay between government and industry. Almost a decade ago, when the Soviet Union collapsed, Europeans were asked how they felt about the United States being the world's sole superpower. Their response: the United States may be the only military superpower, but it is economic power that will rule the new world order.[13] This shift was not lost on the United States Government, which has formally recognized that economic prosperity is key to national security.[14] Put another way, we have elevated economic and market issues to a level previously reserved for matters such as nuclear proliferation. Expanding the government's sphere of concern in this way certainly has implications for government-industry relations, not the least of which is determining how responsibility and control of the nation's critical infrastructures should be shared.

In the past, the government's role and responsibility was more clearly defined: the government was tasked with protecting public safety and national security, using funds collected from citizens through taxation. Although it of course promoted economic prosperity as well, its efforts in this area did not require sacrificing other vital interests. In this classical model, industry was—like any person or entity—a potential victim, with its primary concern the prevention and detection of white-collar offenses. Clearly, a market-based approach to public safety and national security would never work, as these functions cannot be conducted on an economics based cost/benefit analysis where the key metric is "return-on-investment."

In the new digital economy, this tax-funded approach no longer dominates. The government, reluctant to regulate the Internet and risk stifling innovation, has repeatedly stated that the private sector is primarily responsible for protecting the nation's critical infrastructures. After all, the argument goes, it is the private sector that is designing, deploying, and maintaining our computer networks. Thus, the government concludes, critical infrastructure protection requires a public-private partnership, with industry in the lead.[15]

But by allowing industry to lead, the government has in large part ceded public safety and national security to markets.[16] Although such a non-regulatory approach certainly appeals to corporate America, it cannot be forgotten that these private sector entities' primary mission is not to protect public safety and national security, but to protect and increase profitability. This is not to say that public safety and national security concerns are irrelevant to the business community. In fact, attacks on their network may jeopardize customer and investor confidence and adversely affect economic performance. Moreover, most companies genuinely possess a social conscience. But at the end of the day, supporting public safety and national security concerns must understandably be subordinate to a company's primary financial mission as it is economic suicide to operate at a loss no matter how important a capital expenditure may be to public safety. In sum, industry efforts to protect public safety, national security, and, for that matter, their own infrastructure are necessarily circumscribed by markets.[17]

This situation becomes even more complex when privacy is brought into the mix. Because of the ad hoc way privacy laws have developed, law enforcement's ability to access data and, relatedly, a person's privacy, may be dependent on technological choices that have nothing to do with the core values we are attempting to protect. For example, both cable companies and telephone companies provide Internet service, yet each industry is governed by a different set of rules regarding the disclosure of customer data. This has created uncertainty in determining the proper standards to apply when the release of data is warranted: should The Cable Act control, or the Electronic Communications Privacy Act (ECPA)?[18] Similarly, even under ECPA, the predicate that law enforcement must show before obtaining a wiretap order for intercepting voice communications (the commission

of a specifically designated federal offense) differs from the predicate that must be established for interception of electronic communications (any federal felony).

Another non-regulatory example—one that integrates the concerns of privacy, markets, and public safety—relates to the data retention practices of service providers, both in America and in Europe. For marketing purposes, some providers may wish to keep transactional data (data that reflects connectivity by users). On the other hand, privacy concerns put a different pressure on the market; specifically, markets may choose to offer anonymous accounts or accounts—whether anonymous or not—where no transactional data is recorded. At the same time, privacy directives in Europe, such as the Telecommunications Directive of 1997, require European Union nations to pass domestic legislation that prohibits telecommunications providers from keeping data after a bill is paid or the time to contest the bill has passed.[19] The implications of these forces on public safety and national security are enormous. If there is no historical data, it may be impossible to solve any past computer crime, even one only minutes old. Instead, a computer crime would have to be traced back to its source in real-time as it is occurring. In many if not most cases, this will be impossible. For example, if multiple governments are involved (e.g., international hacking), it will be impossible to move through multiple sovereign judicial processes fast enough to get to source while the hacker is on-line. Even domestically, federal law currently requires that an order be sought in every judicial district where data is required from a service provider, even though each court is merely reaffirming the order of a prior court that the legal threshold for compelling the production of data has been met.

Finally, there is the hot topic of the day: "Carnivore," the Federal Bureau of Investigation's new packet-filtering program. Putting visceral reactions to the name of this network forensic tool aside, it is again necessary to think carefully about the impact of technology on public safety. In the old circuit switched network, a wiretap order identified the telephone line to be tapped and agents listened only on that line. Once a call was determined to fall within the scope of the order, the call would be recorded as it streamed across the wire.[20] By contrast, the Internet is packet-switched, and a single communication—even a pertinent one—is broken up into pieces and sent across the network piece by piece. Significantly, each piece is moving down a channel shared by other individuals whose packets are also moving down the same path. Thus, if law enforcement were to capture every packet in that channel, they would capture not only the communications described in the court order, but packets of the innocent as well.

How, then, does law enforcement capture only those packets that the court order authorizes them to intercept? The packets must be filtered as they stream across the channel, using information in the packet to separate those covered by the order from all others. That is what Carnivore is meant to do. The key is that packets not identified in the court order must not be viewed by human eyes, should not be saved in any form, and must not be retrievable. Moreover, the entire process should be audited.

I do not dismiss lightly the argument that Carnivore should be banned because law enforcement will abuse the technology; certainly law enforcement sometimes behaves improperly.[21] But to ban Carnivore on this ground makes no sense, and those who rely upon "government distrust" as the foundation of their argument against the tool fail to see where it leads. First of all, society has already recognized the value of, and condoned the used of, wiretapping. To the extent we resist the development of tools to ensure the continued efficacy of this tool in a new technological environment, we have allowed technology to dictate social policy. Second, to the extent law enforcement is not to be trusted with necessary tools, the answer is not to prohibit the tools and render law enforcement ineffective, for then we fund law enforcement with no appropriate return on investment (i.e., we pay for, but do not receive, a particular level of public safety). The better approach is to develop appropriate controls that ensure the proper use of law enforcement techniques.

As issues such as Carnivore arise, the more appropriate debate, I believe, revolves around whether the gains in public safety are worth the cost in privacy, remembering that we have no usable formula for answering that question. For example, society could create law enforcement and protective systems that are highly, if not perfectly, efficient—such as cameras that catch every speeder on every road but keep no record of the law abiding—but who would want to live in such a society, even assuming that such a scheme passed constitutional muster? As information technology proliferates, we will constantly be confronted with such choices, and that is why we need to rethink the balance between privacy, markets, law enforcement and national security.

CONCLUSION

As criminals gravitated to the Internet, theorists debated whether computer crime was new or merely old wine in new bottles. The answer has become clear: not only are traditional crimes more difficult to investigate in a global and anonymous Internet, but many of our laws, procedures, and organizational structures are outdated. Our inability as a society to meaningfully address major security violations will undoubtedly serve as a catalyst for change, but change itself brings its own risks. As citizens, we demand it all: privacy, free markets, public safety, and national security. Reflective of the complexity of the Internet age, however, these goals are at the same time compatible and contradictory. For example, encryption can at one moment protect privacy, support

commerce and prevent crime, yet at the next moment protect a criminal from prosecution after he has violated the privacy of others by downloading their financial information to commit fraud.

Faced with this conundrum, it is time to methodically reconsider how to balance our contradictory objectives in a data rich, sometimes anonymous environment. We must revisit our legal, economic, and social regimes, rethinking how we protect data, promote economic growth, ensure the effectiveness of law enforcement, and respond to an attack when lacking critical decisional facts. Perhaps hardest of all, we must reclaim our right to strike this balance, and not let markets dictate our choices. That may seem like a simple and sane principle, but it has drifted away. In a recent decision striking down a statute prohibiting commercial Web publishers from allowing minors to access harmful material on their sites, the Third Circuit wrote, "we are forced to recognize that, at present, due to technological limitations, there may be no other means by which harmful material on the Web may be constitutionally restricted."[22] Put another way, the court held that since technology provides no way to protect children, children may not be protected. Although cast as a technological result, technologists develop products based upon the demands of the marketplace. With all due respect to capitalism, society—and not the marketplace alone—should determine how our core values are implemented. ■

FOOTNOTES

[1] According to Forrester Research, consumer may spend $3.2 trillion over the Web in 2003. See USA Today, August 23, 2000, p. 3B.

[2] See generally, "The Internet, Consumers and Privacy," by Ellen Alderman and Caroline Kennedy, an earlier paper in this series and available online at www.internetpolicy.org, and Principles for Providing and Using Personal Information, available at http://www.iitf.nist.gov/documents/committee/infopol/niiprivprin_final.html.

[3] Richard Power, "Current and Future Danger, A CSI Primer on Computer Crime & Information Warfare" (1995).

[4] Carter, David and Katz, Andra, "A National Survey on Computer-Related and Technology Crime." See also, The Washington Times, October 25, 1995, Page B-9 (describing survey).

[5] In one case, a country singer's hospital record was taken for sale to a tabloid. In another case, the search of a hacker's computer revealed over 3,000 prescription records downloaded from a local pharmacy.

[6] At the risk of grossly oversimplifying a complex debate, encryption pitted law enforcement and national security personnel (who wanted to ensure continued access to the plaintext of transmitted and stored data) with high-tech businesses and privacy advocates (the former wanted to sell cryptography products globally, the latter wanted encryption widely deployed to protect privacy). For a more detailed discussion of this debate, see "Codes, Keys and Conflicts: Issues in U.S. Crypto Policy," Association of Computing Machinery (ACM), June 1994 and National Research Council, "Cryptography's Role in Securing the Information Society," (1996).

[7] Historically, states protected "state secrets," not economic proprietary data. In the new world order it is economic power, not military power, that rules. Thus, steps have been taken to protect proprietary information in ways previously reserved for classified information, such as passage of the Economic Espionage Act on October 11, 1996. 18 U.S.C. § 1831 et. seq.

[8] Cf. The Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510 et seq. (establishing rules for wiretapping in criminal investigations) with The Foreign Intelligence Surveillance Act, ("FISA"), 50 U.S.C. § 1801 et. seq. (establishing rules for wiretapping in counterintelligence investigations).

[9] Not only have we distributed this powerful technology, but we have exacerbated matters by deploying it backwards. With most powerful technologies, we give it to adults first, and expect them to teach their children to use the technology responsibly. Automobiles and guns are just two examples. With computers, we have given children powerful technology that their parents and teachers do not understand.

[10] The attack was first detected when the United States was gearing up for potential air strikes against Iraq, and appeared to be coming from the Middle East. Ultimately, the attacks were traced back to two juveniles located in Cloverdale, California.

[11] Under 18 U.S.C. 1030(a)(2), whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any department or agency of the United States is guilty of a misdemeanor. This offense rises to a felony if (1) the crime was committed for purposes of commercial advantage or private financial gain; (2) the crime was committed in furtherance of any criminal or

tortious act in violation of the Constitution or laws of the United States or of any State; or (3) the value of the information obtained exceeds $5,000. 18 U.S.C. § 1030(c)(2)(B). Additionally, 18 U.S.C. § 1030(a)(3) prohibits trespassing in a government computer, even if information is not obtained.

[12] In a case where the activity might involve espionage, parallel criminal and counterintelligence investigations can be run, but this poses its own problems. For example, certain information cannot be shared between law enforcement and the intelligence community, thus ensuring that the left hand does not know what the right hand is doing.

[13] Face The Nation, Sunday, September 8, 1991. Garrick Utley, Commentator.

[14] In a February 25, 1997 speech before the the National Security Industrial Association, William A. Reinsch, Under Secretary Of Commerce For Export Administration, noted that "The world is clearly changing rapidly. Economic goals have become much more important to industrialized nations, turning allies into competitors. That is one reason why this Administration has emphasized economic strength and global competitiveness as a critical element of national security..." (Available at gttp://www.bxa.doc.gov/press/97/War2-25.htm).

[15] See Report of the President's Commission on Critical Infrastructure Protection, available at http://www.ciao.gov/PCCIP/report_index.html.

[16] The public safety argument should be intuitive since attacks on networks are themselves crimes and may have additional public safety effects (e.g., a telecommunications attack may disable 911 services). The national security argument flows as follows. Weak computer security may allow miscreants to incapacitate our critical networks—such as telecommunications, banking and finance and transportation—causing severe economic harm. If economic security equals national security, then economic disasters caused by cybersecurity failures impair our national security.

[17] Cf. The Cable Act, 47 U.S.C. § 551(h), with the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510 et. seq. It is also worth noting that, in today's global environment, a company's allegiance may not be to the United States, but a foreign power. In such situations we are not only ceding our national security to markets, but perhaps to a competitor or even an adversary. For example, allowing a foreign, state-owned telecommunications company (or even a privatized telecommunications company with close ties to the state) to buy a company that provides phone service to the United States Congress would provide a foreign state with the means for direct access to internal Congressional communications.

[18] One of the most peculiar results of this scheme is that if law enforcement is seeking records regarding a cable subscriber, they must notify the subscriber that he/she is under investigation, and there is no provision allowing a court to delay notice. Thus, a criminal utilizing a cable Internet provider must arguably be notified when he/she is under investigation. Cf. the Electronic Communications Privacy Act, 18 U.S.C. § 2705 (notice can be delayed by court order).

[19] In cases of free Internet access, this may mean that no data can be preserved at all.

[20] A process called minimization requires agents to stop listening if the call is not pertinent, subject to spot checks to make sure the topic of a conversation has not changed and now relates to criminal activity.

[21] Lapses in character and judgment are not unique to the law enforcement profession. Doctors sometimes abuse narcotics, accountants may steal money, and individuals too frequently drive while intoxicated.

[22] ACLU v. Reno, 2000 U.S. App. LEXIS 14419 (3d Cir. 2000)(striking down Child Online Protection Act).