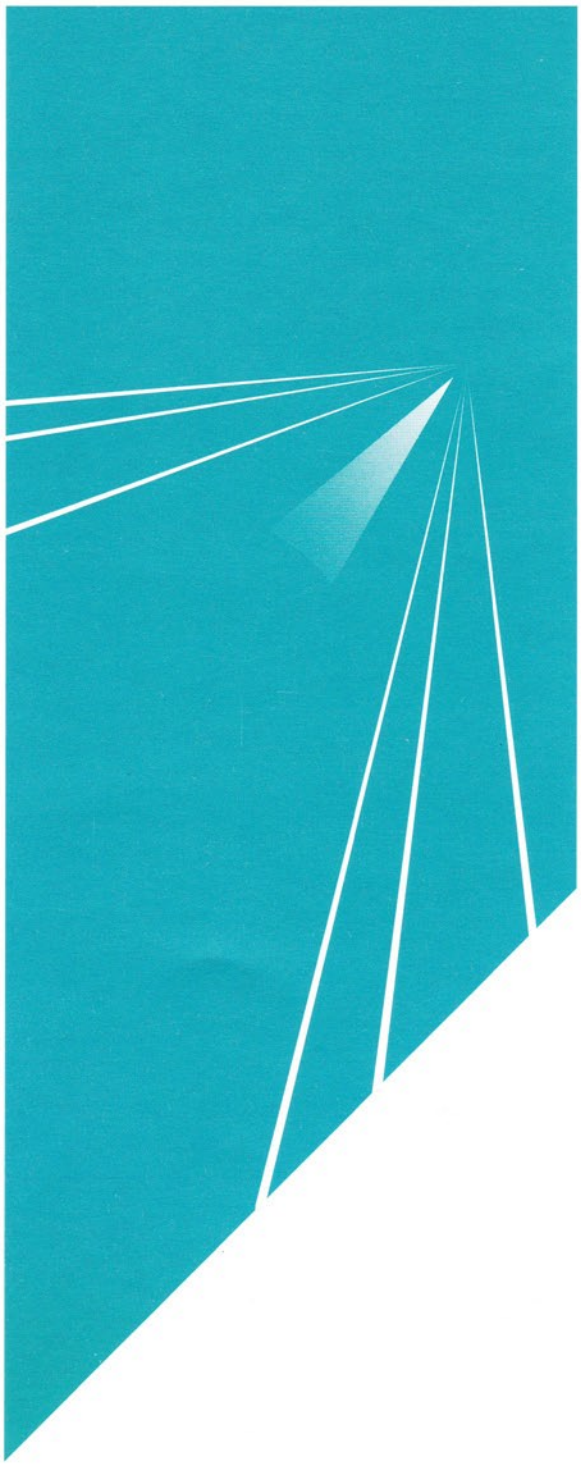


Position Paper

Five Privacy and Security Imperatives for Electronic Trade

by Larry Downes

with commentary by
John Perry Barlow

CSC

CSC | vanguard

April 1995

Five Privacy and Security Imperatives for Electronic Trade

Views on the February 1995 Vanguard Conference, "Privacy and Security: Keys to the Electronic Trade Exchange"

by Larry Downes

CONTENTS

Position Papers provide strong viewpoints on critical technologies, applications, or management issues identified by Vanguard principals, or that surface as important concerns during Vanguard meetings. Written by one or more Vanguard principals, Position Papers offer in-depth analysis, opinion and recommended actions where appropriate. For additional copies, please contact Lani Stiles at (617) 499-1574.

About the Authors

Larry Downes

Vice President, CSC Vanguard

Larry Downes has a diverse background in technology strategy, large-scale information systems development and integration, and intellectual property law, all with an emphasis on emerging technologies and their affect on business strategy. With 10 years in management consulting, his responsibilities have included worldwide practice management for artificial intelligence and mid-range systems, and development of technology strategies for leading information technology companies. Mr. Downes, who holds a law degree, has experience in intellectual property issues and financing for technology companies. He welcomes comments and further discussion via e-mail at *ldownes@csc.com*.

John Perry Barlow

Co-Founder, Electronic Frontier Foundation, and Advisory Board Member, CSC Vanguard

John Perry Barlow is a retired Wyoming cattle rancher, a lyricist for the Grateful Dead and co-founder of the Electronic Frontier Foundation. The Electronic Frontier Foundation, founded by Mr. Barlow and Mitchell Kapor in 1990, is an organization that promotes freedom of expression in digital media. Mr. Barlow is a writer and lecturer on subjects relating to the virtualization of society. He is a contributing editor for numerous publications, including *Communications of the ACM*, *Microtimes* and *Mondo 2000*. He is also a contributing writer for *Wired*. He is a recognized commentator on computer security, virtual reality, digitized intellectual property, and the social and legal conditions arising in the global network of connected digital devices. Mr. Barlow lives in Cyberspace at *barlow@eff.org*. Visit his home page on the World Wide Web at *http://www.eff.org/homes/barlow.html*.

Most of the people referred to in this paper participated in the Vanguard conference, "Privacy and Security: Keys to the Electronic Trade Exchange," held February 2-3, 1995. See appendix.

Five Privacy and Security Imperatives for Electronic Trade

Views on the February 1995 Vanguard Conference, "Privacy and Security: Keys to the Electronic Trade Exchange"

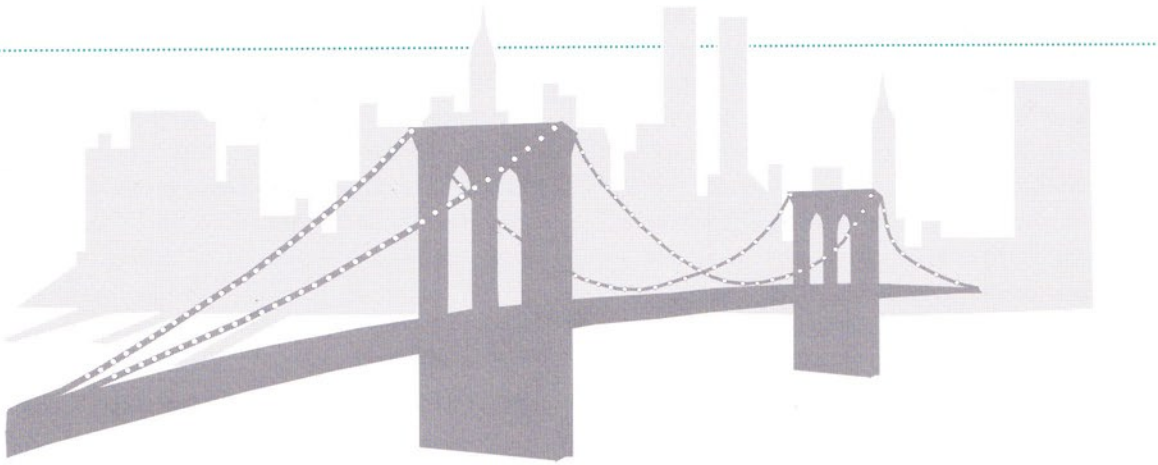
by Larry Downes

"You can no more reason from highway precedents to railway problems than you can reason from the ox to the electric battery."

— Brooks Adams, historian, 1895

"Sociology is a very interesting subject."

— Alan Kay, technologist, 1988



Roebling's Bridge

The instinctual response to the idea of using today's emerging communications networks (generally, "Cyberspace") as a vehicle for doing business is a visceral one or, as Vanguard advisory board member John Perry Barlow says, an immune response:

> "The Internet is not secure, and until it is, I won't do business there."
>
> "Electronic commerce will not develop without strong cryptography."
>
> "I would never give my credit card number out over the Web."

It is worth acknowledging that these *are* visceral, instinctive responses. When the Brooklyn Bridge was built just over 100 years ago, it employed many new technologies that enabled John Roebling to create the world's longest suspension bridge. It was the first such bridge across the East River, and dramatically expanded the effective (or virtual) size of New York City. Since the main support for such a bridge is invisible, buried deep in an anchorage, Roebling's design *looked* impossible, unstable and dangerous. (It still *looks* that way, but we have learned to ignore it, just as we have learned to ignore the fact that the sun appears to revolve around the earth.) Many at the time doubted such a structure could be sound, and a week after it opened a rumor spread that the bridge was collapsing, causing a riot among the throngs of pedestrians crossing between Manhattan and Brooklyn. Twelve people were killed.

They were not killed by the failure of the bridge.

Large-scale semipublic networks are the suspension bridges of today. We can't see how they are held together, and no matter how carefully the physics of such structures are explained to us and their tolerances and risks calculated, there is a psychology, a group psychology, that does not want to believe such networks can stand. Where are the firewalls, the encryption algorithms, the provable

specifications for a secure operating system – whatever these things are?

It is not to discount the real business issues involved in operating in Cyberspace to acknowledge that human psychology fears the unknown. We hear the nightmare stories of Tsutomu Shimomura and Cliff Stoll, and wake up in a cold sweat. Someone is methodically, indeed mechanically, poking around in our house and our office and our colleagues' offices, and when he finds anything at all, he picks it up, reads it and discards it. The intruder is unrelenting, cold, invisible. We all experience the victim's very real sense of having been invaded, violated, exposed, humiliated. The Internet Worm. The Good Times Virus. The Invasion of the Body Snatchers. Be afraid. Be very afraid.

It is also not to discount the realities behind these and many other stories – some of which won't be told because the victims have good reasons, both personal and fiduciary, not to speak, and others, even more frighteningly, because the victims never knew they were attacked – to recognize what psychologists call cognitive dissonance. We believe that we are innately able to weigh risks against benefits. But we are wrong. Studies have shown that humans in fact tend to overestimate risk based on anecdotal data, perhaps as a function of natural selection. To augment Vanguard advisory board member Bob Lucky's example, we hear of a terrorist bombing in Paris some years ago and decide not to visit Europe; instead, we get in the car and drive to the corner store without our seat belts on. No matter how much proof we are given that the risks of death from the latter are astronomically higher than from the former, a part of us does not want to believe the truth: that we are far more likely to be injured by the innocuous and mundane threat than we are from the dramatic and newsworthy. It defies our ego to believe that we could be harmed by anything smaller than we are.

Armed with this powerful psychological insight, we have identified five privacy and security imperatives for companies considering entry into or large-scale expansion of electronic trade.

Five Imperatives for Electronic Trade

1 *Don't Trust Your Instincts in Evaluating the Risks of Operating in Cyberspace.*

The wise person will use psychology as a competitive tool. He recognizes that our natural response to new technologies is fear – literally, a feeling of insecurity. He understands that competitors will overestimate risks; will let opportunities pass them by; will play it safe when staring at a brand-new marketplace or channel, or a new way of reducing the transaction costs of doing business, or a new way of forming relationships, or creating new forms of corporate entities. He listens while others say the Internet is not secure and encourages them to believe this is so and that it is relevant. Meanwhile, he is busily weighing the real risks and comparing them to the real benefits, getting ready to make a strategic move.

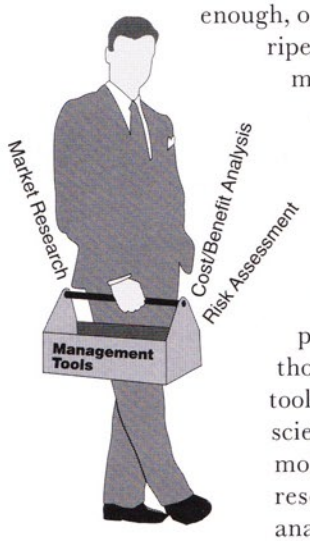
He might, for example, approach two of the thorniest issues of security in Cyberspace – transactional security and firewall breaches – in the following context:

- **Transactional security.** Everyone knows that it would be foolish to give out credit card numbers over the Internet. Never mind that we give these highly secure codes to total strangers all the time, sometimes over the phone to organizations we haven't the slightest reason to believe are really legitimate businesses, or to order takers who have no incentive not to sell the information or give it away immediately to some bulletin board. Never mind that we have no liability as consumers for unauthorized purchases (including, whether by law or custom, the $50 we think we have to pay because we're told that this is our "maximum liability," largely to make us more diligent on behalf of the card services). Never mind that, as merchants, we are similarly protected by the card services; indeed, that is why we pay transaction fees. Never mind that the banks and other financial service providers have every incentive to develop sensitive authorization techniques to minimize the actual risk of fraud and that, by and large, they already have.

- **Firewall breaches.** We all fear establishing a presence on the World Wide Web because of the risk that intruders will break into our private networks. Just one terrorist (whether it's Saddam Hussein or – worse, it seems – an ingenious adolescent) can erase all of our company's information assets, so there's no point in even evaluating the potential revenue that could be generated, or the costs improved, or the competitive barriers erected, by establishing such a presence. Never mind that we run the same risk every time we hire (or fire) an employee, or allow a contractor or vendor access to our systems. Never mind that we have an inadequate security organization in place now, or an outdated disaster plan. Never mind that we haven't really evaluated our exposure since a time long before operational data was even present on our computer systems. Never mind the damage that can be done inadvertently by the cleaning staff.

As Steven Levy points out, we used to think of "hackers" as the heroes of the information revolution. Now we think of them as, well, revolutionaries. Who changed?

The point is not that there are no risks, or that the Internet is secure enough, or even that the time is ripe for moving our entire mainline business activities to Cyberspace. The point is that now is the time to evaluate these opportunities as rational business people, armed with all those low-technology tools: management science, financial modeling, market research, cost/benefit analysis, risk assessment.



We need to quantify our fear.

There's no magic to making money in Cyberspace. Magic is the thing we're afraid is out there. We trust in the international telephone networks, the automated teller network, the air traffic control system, the real-time monitor in our home thermostat, and dozens of other insecure (and worse, buggy) systems, not because there are no risks of serious damage, but because we have enough data points to weigh the risks against the benefits of using such systems. We need to begin collecting data points in Cyberspace and determining what are the real risks. Then we can decide if the privacy and security protection choices available are good enough.

2 *Don't Look to the Federal Government for Help – or Anything Else – in Cyberspace. And that's the Good News.*

Despite the fact that the government was the chief sponsor of all the basic technologies critical to current information technologies (including what is today known as the Internet), waiting for Washington to roll out the National Information Infrastructure – or to establish standards for secure, cost-efficient allocation of Cyberspace's bandwidth, or to rationalize the current morass of statutes and regulations that make up the export controls, intellectual property, and the criminal code – is waiting for Godot.

Ray Kammer's exegesis of the current administration's policy regarding encryption and "related activities" suggests a government that is at best hallucinating and at worst irrelevant, if not the other way around. The government's policy is to limit the use of technologies the government acknowledges are critical to the success of electronic commerce, specifically by prosecuting the export of cryptography. But don't worry, says the government, the government will fail. The administration's fifth policy statement, according to Kammer, proclaims flexibility on encryption approaches: "We actively seek additional solutions to these difficult problems." In other words, "We're from Washington. We're here not to succeed in our efforts to get in your way."

Clinton Administration's Cryptographic Policies

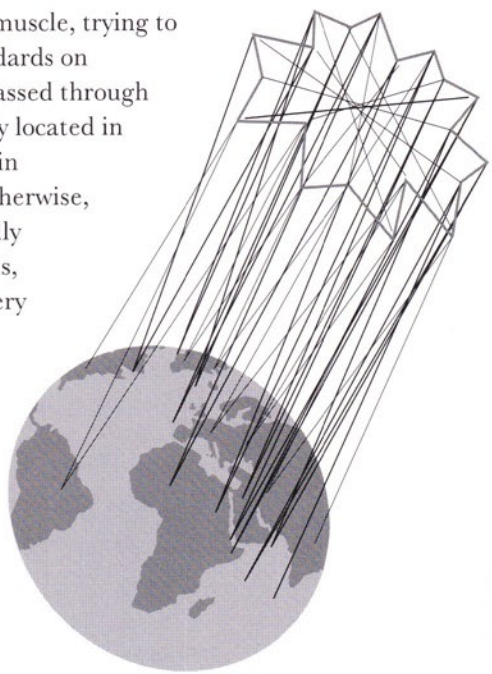
1. Encryption is an important tool to protect privacy and confidentiality.
2. No legislation restricting domestic use of cryptography.
3. Export controls on encryption are necessary but administrative procedures can be streamlined.
4. The government requires a mechanism to deal with continuing encryption policy issues.
5. The government supports flexibility on encryption approaches.
6. Use of the Escrowed Encryption Standard is voluntary and limited to telecommunications.
7. Government standards should not harm law enforcement/national security.

Source: Raymond Kammer, U.S. Department of Commerce

Or consider the administration's seventh policy statement, which is that new technologies, where possible, should not *in any way* inhibit current law enforcement capabilities. But any technology that enhances or otherwise expands the range of human interactions will *always* make law enforcement more difficult. As Whit Diffie pointed out, similar fears accompanied the advent of global telecommunications, yet national governments and the rule of law appear to have survived this and many other decentralizing technologies. But no more, or at least not in a world where government policy is translated into action. "Now let us get this straight, Mr. Bell. Your device would let people in different places talk to each other in private? Have you even thought about the impact that could have on law enforcement? Let us get back to you after we've had a chance to deal with this Mr. Edison." And this is the policy statement of the Department of *Commerce*!

In reality, these policies have no hope of succeeding, and were almost surely designed to be dead on arrival. So the best the government can do is to fail to impede the development of electronic commerce. Surely it will do nothing to encourage it. There will be no Interstate Highway system in Cyberspace. There will be no Erie Canal, no St. Lawrence Seaway, no international air routes, no universal Postal System, no Geneva Conventions. Standards, infrastructure and currency will all be developed by the free market, a Milton Friedman dream come true. For better or worse, Cyberspace will remain an unregulated market, one that operates with almost no transaction costs.

We think this is decidedly for the better. Because it is not only the United States government that wants to regulate, but governments at all levels. Individual states are already flexing prosecutorial muscle, trying to impose their community standards on pornography that may have passed through an Internet host site physically located in their borders. No transaction in Cyberspace, commercial or otherwise, can take place if it is potentially subject to the laws, regulations, ordinances and customs of every minute jurisdiction it theoretically passes through. Because, theoretically, it will pass through all of them. Regulation of virtual space by governments in the physical world would be like introducing air into a vacuum – it wouldn't make it a safer place to breathe, it would destroy it.



Perhaps to ask what the federal government's "role" in Cyberspace should be is as meaningless as asking whether Fred and Wilma Flintstone are married in real life. Maybe Cyberspace isn't in the United States or any country at all, but exists as its own sovereign, virtual nation, and – what may be most chilling of all – that virtual nation might just be the home country of all global businesses. If this is true, Cyberspace needs not only its own markets and customs but needs them in forms suitable to its special nature.

But if Cyberspace is sovereign territory, how can it exist without its own government? How can business be conducted without contract law, protection for intellectual property, police and other law enforcement, currency, taxes, courts? That's anarchy, right? I'm not setting foot in such uncivilized space, let alone do business there.

In fact, the history of commerce is replete with examples of organic, self-governing systems evolving through custom and trade usage. In medieval England, practices developed in the open market evolved into what was known as the law merchant, a set of background rules and principles followed in transactions between merchants. These included agreements as to who bore the risk of loss of inventory ("free on board"), and what terms applied in the absence of specific agreement. When Karl Llewellyn and his New Deal colleagues attempted to unify the hodgepodge of state-specific laws that made U.S. commercial law confusing and disputes expensive to resolve, they recognized the elegance and efficiency of the law merchant and largely adopted it in the Uniform Commercial Code, a single system of commercial law now adopted by every state in the U.S. and by many foreign countries as well. Three cheers for anarchy!

There are already indications that a similar organic form of governance is evolving in Cyberspace, growing out of the general principles of electronic interaction known as netiquette. Some of the earliest incarnations have been crude, like the system operators who pass "death sentences" on misbehaving users, wiping out all traces of their electronic existence. Increasingly, civilized voices like the Electronic Frontier Foundation's David Johnson have proposed virtual mediation – panels of experts convened on the fly – and, where appropriate, electronic democracy.

The wise organization will seize the opportunity to work in an unregulated market that recognizes efficiency and rewards innovation. It will not waste time encouraging the federal government to intervene, which is neither likely nor desirable. Instead, it will use its influence to ensure all governmental activities in Cyberspace remain minimal and ineffective, and focus its efforts on building coalitions and trade groups that will quickly establish Cyberspace's law merchant, including transaction enablers such as digital money, other financial services such as digital notarization, and netiquette.

3 *Think of Personal Privacy as a Commodity, Not an Obstacle.*

It's hard to separate out all the agenda underlying the "debate" regarding personal privacy and Cyberspace. The Electronic Frontier Foundation, following the lead of the Internet community in general, has been portraying this issue largely as a problem of individual liberty, of an insidious Big Brother – particularly his national security incarnations – eager to wipe out the Bill of Rights in Cyberspace before it can take hold.

Some perspective on privacy would be helpful. Historical studies of privacy in the United States suggest that we live in a better and worse world today than, say, the colonial period. The Puritans did not expect their mail to be private, but they did expect that their bedrooms were. So privacy is not a static concept, and law enforcement insistence on maintaining "parity" with new technologies has it exactly backwards. Parity arguments ignore the fact that new technologies have created new forms of human interaction, leading to unhelpful metaphysical questions like whether e-mail is the "type" of communication the government would "traditionally" have been able to intercept without a warrant; that is, whether it is more like an overheard conversation on the village green (not private) than pillow talk (private). For the past 50 years, the Supreme Court's non-test has been to ask whether the speaker had a "reasonable expectation" of privacy.

But is the government really who we need to be protected from, or even the only entity we should fear? On the other side are the dangerous hackers breaking into the machines of many of our speakers, wreaking havoc. It's not cool, says Tsutomu Shimomura, to read other people's e-mail, whether it's a hacker or, we can add, the government. After playing for us the eerie tape of phone mail messages from the hacker who ripped off his files, Tsutomu went off to assist the FBI – that's the government, mind you – in capturing a suspect in the case, a notorious figure named Kevin

The View from the Brooklyn Bridge

In response to "The Five Privacy and Security Imperatives for Electronic Trade"

by John Perry Barlow

Co-Founder, Electronic Frontier Foundation, and Advisory Board Member, CSC Vanguard

Just last week, I took a Dutch friend on a walk across the Brooklyn Bridge and submitted her to an extemporaneous lecture on the parallels between that literal and genuinely religious leap of faith in 19th-century American engineering and the Internet as the current manifestation of the same wild thrust, engendering some of the same popular anxieties.

I told her that I thought the decade in which the bridge was designed and largely built, the 1870s, was a decade which in some ways resembles the present. It was a time of shattering invention and originality. Many of the technologies that would utterly alter us during the intervening century – the telephone, commercial electricity, sound recording and steel construction – exploded into the world.

It was another time when engineering suddenly endowed us with apparently limitless potential. The prophets of that time – from Marx to Edison to the Roeblings, father and son – were as feverish with the inevitability of their visions as the Tofflers and cypherpunks of the present. And, as Larry says, many of the ordinary folks were scared to death of a future they could neither prevent nor understand.

As symbols, though, there are some important differences between the Brooklyn Bridge and the Internet, many of them related to the sources and advantages of faith. These were brought into sharp focus at Vanguard's privacy and security conference in Palm Springs, and I've been mulling them over ever since.

Faith in the Known

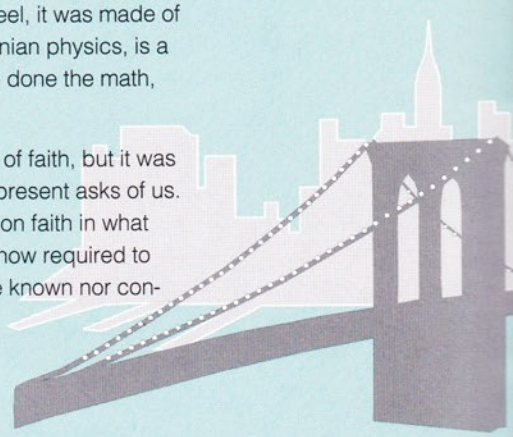
The Promethean engineers of the 19th century were thrust upward on Toffler's Second Wave at the time of its maximum velocity. They were in a matrix of progressive zeal that spread from the crisp vertices of Descartes to the vanishing points of Manifest Destiny. They believed in Control, and, of course, Almighty God, by whom Control had been ordained and in whose name it was imposed.

The Roeblings' bridge may have terrified the *hoi polloi*, but to the men who financed it, it was a reasonable statement of faith in physics – the most dramatic of its time perhaps – but well within the confines of a paradigm that had been bearing steadily increasing fruit since Newton and, in many ways, since Moses.

Further, the Brooklyn Bridge undermined none of the institutions of its day. Indeed, it was part of what was building them. Coming out of an era in which the only large institutions had been religious in the classical sense, it represented both the Church and its new siblings, the Corporation and Large Government. It's no mistake that its arches ascend to an ecclesiastical point.

If you walk across the bridge today, you feel its blunt simplicity. In addition to stone and steel, it was made of physics. And physics, at least Newtonian physics, is a lot simpler than biology. Once you've done the math, you can trust the trajectory.

It was also, as Larry suggests, made of faith, but it was a very different kind of faith than the present asks of us. Where the Brooklyn Bridge was built on faith in what was known and controllable, we are now required to place our trust in what can neither be known nor controlled.



Faith in the Unknown

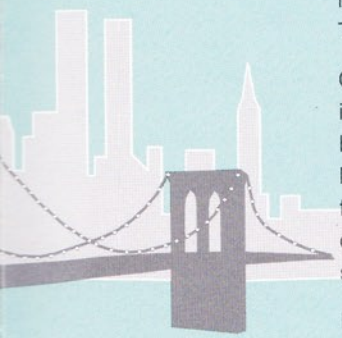
We have left the Machine Age and are plunging into the fogbank of something completely different, the Era of the Organism. The new masterworks of humanity, of which the Net is very likely the most important, are of such complexity that they can no longer be designed and built. Instead they must be grown. It isn't physics. It's biology. It's nature.

There are no smooth, catenary curves in nature. The trajectories of biology are "forky" and unpredictable as lightning. There is a new mathematics to describe them, but what these numbers tell you is only that you can't know where things are headed. It's hard to imagine the Brooklyn Bridge would have been funded had it been designed according to fractal geometry rather than calculus.

The current hurdle of civilization into Cyberspace has required, like the bridge, the assembled acts of the existing institutions, but it hardly reaffirms them. For one thing, a large collective enterprise loves certainty above all other things, including profit.

In the pursuit of certainty, almost any established corporation will follow the Devil It Knows, whether buggywhips or minicomputers, straight to doom. Nothing is certain in Cyberspace but accelerating change. The curves we can plot – processor speed, Internet growth, Web use, bandwidth – are all increasing logarithmically or faster. Furthermore, there is reason to think many of them will become irrelevant in this new environment, devoted as they are to distributing centralized goods and services.

For this reason, it is hardly surprising that many of the corporations that were putting us up in this hotel at the corner of Dinah Shore Drive and Bob Hope Way resist going into Cyberspace. In some deep, organic recognition of their own, they know there be dragons there. They have a sense of nameless dread.



Of course, dread hates to be nameless so, in this instance, it finds its focus in the Nightmare Hacker, bent on lobotomizing corporations for the hell of it. Never mind that there is no evidence with which I'm familiar that this beast actually exists. He is a creature of the unfamiliar. The premise that he *could* exist is sufficient reason to stay out of this mysterious realm.

If corporations must go into Cyberspace, they insist on doing so with certainty and control assured. They want the government to send in troops first and ferret out such guerrillas as Kevin Mitnick and his kind. They want to establish the predictable rule of law. But this isn't Panama. It's more like Vietnam but worse, since the threat is largely imaginary (and thus impossible to contain). It's also worse because this jungle is infinitely expansible, and worse still, it's not even clear whose troops should go in or whose law should reign.

Faith in Openness

This relates to one of Larry's statements that I found telepathic: "Maybe Cyberspace isn't in the United States or any country at all, but exists as its own sovereign, virtual nation, and – what may be most chilling of all – that virtual nation might just be the home country of all global businesses." When I read this line, I was fresh from giving a speech at the Technology Entertainment Design (TED) conference in Monterey in which I had proposed precisely that.

In the created world that arose from Newton, power was derived from closed architectures of one sort or another. Creating wealth was a matter of skillfully managing scarcity and maintaining clear boundaries. But the natural world favors open systems. Indeed, it requires them, since the energy exchange processes upon which it builds its increasing layers of complexity must be interoperable in the deepest sense of the word. The Net is no different.

As I listened to Bill Cheswick, I realized that he was describing a system of such perfected security as to be fundamentally incompatible with the requirements of both the Internet and the World Wide Web, both of which need highly permeable membranes in the systems that make them up. The only way they can interact properly with their environment and maintain the security of their contents is through the internal use of cryptography, but this is another technology that existing institutions find threatening.

Then there are the threats to the control of intellectual "property" upon which many existing institutions have based their sense of well-being. If they cannot assure their ability to "own content," and there is no longer a business to be had in putting their intellectual property into objects and shipping it around in trucks, then what will they do for a living? Hard questions.

But can anyone not explicitly involved in the local manufacture of physical goods expect to be successful without entering this great region of ambiguity? I don't think so. We are at one of the great watersheds of history, a more momentous moment than the Brooklyn Bridge. All of us, whether individuals or institutions, will be required to make enormous acts of faith and leave our old beliefs at the border. Those who can't will be left behind.

But where the Brooklyn Bridge required of its builders faith in their ability to control technology, going into Cyberspace demands a much purer form of faith: faith *without* control. Faith in nature. Faith in *human* nature. Faith that what goes around really *does* come around. Groundless faith.

But I have often suspected that groundless faith, like unconditional love, is the only kind there is.

Mitnick who had already seen jail time for his hacking activities. The story received tremendous coverage, including a series of articles by John Markoff in *The New York Times* and commentary from Steven Levy in *Newsweek.* Tsutomu was seen skiing, at last, on CNN.

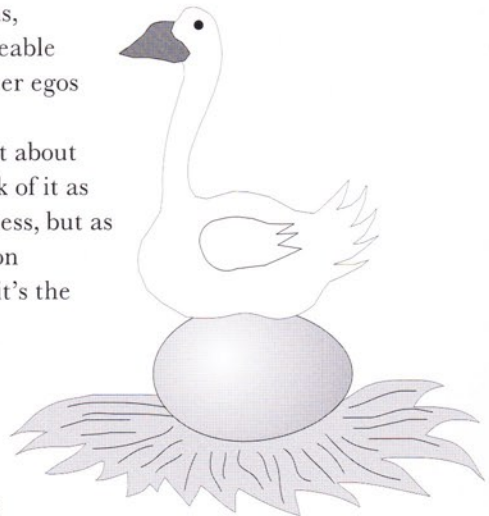
We take a certain pride in our colleague's catching up with his tormentor. But now in the aftermath, one must ask if the federal time that Mitnick is likely to serve for his exploits is a punishment that fits the crime. Andrew Shapiro, reporting in *The Nation,* acknowledges a strong backlash developing in the Mitnick case, including criticism of Markoff's personal involvement in the search. "Mitnick didn't steal money, he didn't hurt anybody," says *2600 Magazine* Editor Emmanuel Goldstein. The credit card numbers he had are also in the possession of many other hackers, and they haven't used them. Information, say the hackers, wants to be free. And boys, it seems, just want to have fun.

So are hackers the spoilers of Cyberspace, or are they its guardians? Is the FBI the agency of choice for tracking down those who interfere with our electronic commerce, when it is their Byzantine cryptography policies that keep us from being able to secure the environment in the first place? As Patrick McGoohan used to say on the old "Prisoner" TV series, just who are the prisoners here, and who are the guards?

Maybe these aren't even the right questions to begin with. One of the most poignant moments of our conference came during John Perry Barlow's session, when a sponsor asked him why it was that he and his colleagues were so concerned about what seemed to be an incompetent government, rather than a commercial sector with more history and much more incentive to invade personal privacy. A sobering question. We give away incredibly private information about ourselves all the time to hotels, airlines, video stores, creditors, grocers, and the like. And whatever the state of a citizen's "right to privacy," in the United States and elsewhere, it has never been thought to apply to non-governmental actors. Even those who would protest the loudest against a national identity card happily carry dozens of magnetic stripes in their wallet, fill out forms at the drop of a hat, and allow their groceries to be scanned. There are few laws limiting the use of such information. For $15, credit bureaus will sell you the privilege of cleaning up their data about you.

In Cyberspace, even more information about you will be available – and at virtually no cost – to create, distribute, merge, sort and replicate. So the invasions of privacy will be that many orders of magnitude worse, right?

Wrong. While the technical barriers to massive data collection, consolidation and disbursement are evaporating, so are the barriers to voicing collective mores about what is or isn't "reasonable." Traditional barriers to collective action are also overcome in the low transaction cost environment of Cyberspace, making it possible for the "market" to be truly responsive, rewarding good practices and punishing bad ones. Quickly. Widespread corporate abuse of private data will not be tolerated. Organizations that misuse data can and will be punished in the worst possible way – economically. And where there are markets for anonymous transactions, ingenuity will provide solutions, whether in the form of untraceable currencies (digital cash) or alter egos (intelligent agents).



The more important point about personal privacy is not to think of it as an impediment to doing business, but as an enabler. Personal expression stimulates economic activity; it's the goose that lays the golden eggs. Rather than worrying about which of our marketing efforts will offend privacy watchdogs, we should instead be thinking about ways in which we can use Cyberspace to encourage new forms of expression and communication in a secure and comfortable environment. Focus on the product, in other words, and use common sense in the design of the store.

The wise organization will closely monitor attitudes and behaviors of the residents of

Cyberspace, just as they do in the physical world, but will get much clearer and much more timely feedback from the market. Market research and advertising in Cyberspace, as well as strategic planning, production scheduling, product design, inventory control and financial planning, will become much more (more?) scientific. The successful organization will go further, recognizing, as Vanguard advisory board member Nicholas Negroponte says, that transaction data is worth little without knowing how the customer felt about the transaction. In the accelerating pace of modern life, both buyer and seller will need to find each other quickly and effortlessly. Services like ProductView Interactive's online advertising service, which links buyers to sellers, will do just that. ProductView recognizes the value of the consumer's personal information and handles it gingerly. ProductView creates explicit economic incentives for consumers to share their information with others, but won't share that information unless the consumer grants permission. However, as electronic commerce encourages greater intimacy with consumers, they will want to provide private information because doing so will make their lives better. That, at least, should be our goal.

4 *Before You Start a Vigorous Exercise Program, See Your Doctor for a Check-Up.*

As Bill Cheswick says, "The Internet is a bad neighborhood." It's a landscape of dark alleys, populated by shady characters wielding menacing objects. UNIX is a grossly insecure operating system, as are MS-Windows and the MAC/OS (according to David Bauer, they are inherently so). Perhaps only 1% of all attacks are even detected, let alone reported. And so on and so on. Tsutomu Shimomura, Cliff Stoll, Bill Cheswick and David Bauer together painted a picture of an insecure, foolish network structure, which yields full ("root") privileges at the drop of a hat. As Whit Diffie pointed out, "In some sense, security exists to *create* interoperability problems." Since, as John Perry Barlow says, the Internet derives its strength from being open and interoperable, perhaps it's no surprise that its system-level security is, to put it kindly, porous. That's how it breathes.

The point has already been made that the actual security risks need to be evaluated in light of both the potential precautions available (Windows NT, cryptography) and the potential benefit to be weighed against whatever risk cannot be eliminated. As Bill Cheswick says, your Internet security policy should emerge from the answers to some fairly basic questions: What are you protecting? What are the threats? What's it cost to protect it? Federal Judge Learned Hand wrote many years ago that a precaution should be taken if and only if its cost is less than the cost of harm that would occur in its absence, multiplied by the likelihood of that harm actually coming into being. It is hoped that the conference provided the beginnings of some data points on the elements of this analysis. To allow sponsors to explore the possibilities of electronic commerce in a relatively risk-free environment, Vanguard intends to provide a testing environment as part of the Vanguard Webcenter.

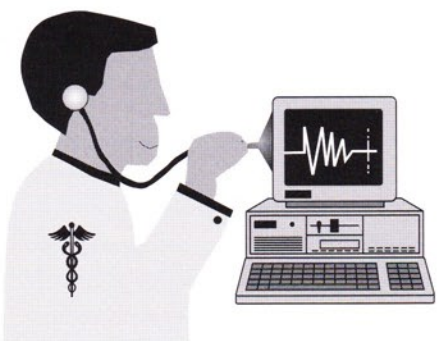
Imperative Number Four is something of an aside, an unpleasant recognition, a dirty little secret many of us share. And that is that our current environments aren't very secure to traditional risks and traditional threats. Our disaster plan has a few inches of dust on it. Our security officer position has remained unfilled for several years. We don't change passwords often enough or, as Bill Cheswick recommends, eliminate passwords altogether. David Bauer says we spend all our money on detecting attacks and nothing on preventing them, but he is probably being charitable. Probably we don't spend much money on detecting either.

For most of us, who have never experienced a true disaster or a major break-in that led to loss of data or disruption of service, perhaps there is nothing especially embarrassing about the current state of our security infrastructure. Perhaps we have, as Judge Hand advised, taken only those precautions that are cost-effective – if the risk of an accident is low, after all, how much precaution is appropriate? As Bill Cheswick points out, with enough money he could bring any system down. (But how much money does it take to break into the national security systems we heard about that still have null passwords for systems operators?)

Whether or not we have done a good job of protecting our networks thus far, and whether or not we have done so by careful planning or serendipity, the point here is that hooking into Cyberspace and increasingly expanding our presence there – including operations, sales, marketing, manufacturing, distribution, research and development, and finance – changes the equation. The change is particularly dramatic for the organization that has been largely isolated from electronic links with itself and its trading partners. The degree of harm increases, as does the probability of its occurring. So even if a minimal security plan has "worked" up until now, it should not be assumed that the same plan will work in the interconnected future. And before committing budget dollars to building the ultimate firewall, or finding the fix to the dreaded IP spoof attack, a more cost-effective and more manageable approach might be to revisit our basic protections first and bring them into the 20th century.

We recommend that as part of any plan to establish an Internet presence, organizations conduct a "health check" or security audit of existing policies and practices. Quickly – and quietly – plug up the holes through which Mack trucks might already fit comfortably. One of the laws of Cyberspace physics must surely be that any weakness in our existing defenses will be amplified and broadcast as soon as we take up residence there. Good news travels, but bad news travels faster.

The extent of the health check, of course, should be determined following Imperative Number One and the basic framework provided by Bill Cheswick and David Bauer. What do you have that needs to be protected? How much is it worth? What are the risks? The answers to these questions should help you determine whether it requires you to consult with the likes of Tsutomu, Bill and David who, as representatives of the government, the common carriers and the investment community, respectively, have the most to lose and consequently have given the problem the most thought.



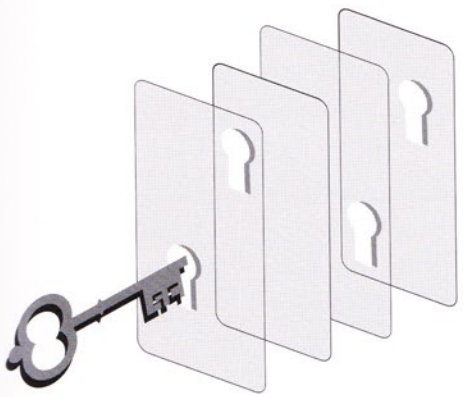
5 *Cryptography Is the Primary Tool. But Don't Use a Screwdriver to Pound a Nail.*

Perhaps the one thing we heard consensus on from the speakers and advisory board members was that cryptography, and particularly public key encryption as invented by Whit Diffie and others, offers the promise to close many of the security holes in Cyberspace at minimal cost, with tremendous reliability, and in a way that perpetuates one of the Internet's best features, which is that it would not require a central authority, sovereign or other, to implement or police. Public key encryption, implemented for example in the RSA algorithm, is a technique whose brilliance resides in its simplicity, allowing senders and receivers to interact with each other securely without first establishing elaborate protocols and protective measures. Everyone can see my public key and use it to send me encoded messages, but only I can decode them with my private key.

Aside from inertia, the major obstacle to a globally dispersed encryption standard based on public key techniques is, unfortunately, the United States government. Officially, Ray Kammer offered us the government's policy reason – national security – for prohibiting the export of encryption technologies, including RSA and DES except in very limited situations and for a small subset of the banking industry (see Imperative Number Two), and for encouraging instead the adoption of a Clipper/Capstone standard, in which the U.S. government holds copies of your private key in escrow. But unofficially, he agreed with

everyone else that: the government will not succeed in cajoling the world into accepting an escrow solution, particularly not when the U.S. government is the self-appointed escrow agent; the government will not succeed in restricting the global export and use of DES; and cryptography is an imperative for electronic commerce. Indeed, those who have implemented Lotus Notes on a global scale informed us that the main reason they have not turned on its built-in encryption feature has been the export restrictions on DES.

So global encryption standards, based on either a public key model (RSA) or a symmetric model (DES), appear to be simply a matter of time and the ebb and flow of competing security and commercial policies along the Potomac. We should do what we can to encourage Washington to abandon policies that it knows are doomed to fail and which it doesn't even believe are in the national interest, at least in the area of encryption export.



In the meantime, now is the time to consider what encryption is good for, and where it makes sense to implement it and where it makes sense not to. As Vanguard advisory board member David Reed says, "Today's credit cards work. Cryptography is for something else." We don't need to add another layer of computation to credit card transactions because there are already adequate security systems in place to preserve them, and the risk of loss is already on those who have the incentive to keep credit cards operating (*e.g.*, the banks and other card service providers). And some transactions, such as large-scale electronic funds transfer, are such obvious candidates for encryption that they are already using it.

But what about transactions in the middle? Should e-mail be encrypted as a matter of general principle? Electronic Data Interchanges (EDI)? Video conferences being transmitted over common carrier lines? Cellular phone calls? As the worlds of cable, cellular, private and public wire, fiber and ethernet, hardware and software vendors converge like mating mosquitoes in an unholy cloud, who should be the providers of encryption services? AT&T? Microsoft? Everybody? Nobody? In which cases is encryption not the appropriate solution, or not the only piece of a secured transaction? As Scott Stornetta pointed out, just because a transaction is encrypted does not mean that it has not been tampered with by the sender. And as David Reed pointed out by way of a corollary, just because an electronic exchange is self-attesting as being authentic and unaltered doesn't mean its contents weren't plagiarized, manipulated, or otherwise incorrect before being notarized. Scott Stornetta agreed that he himself would not do business in Cyberspace without a secured audit trail.

Encryption is clearly a major tool in securing Cyberspace. But it is not the only tool, and it is not appropriate for all types of electronic communications. Perhaps if we can achieve a clearer understanding of where it fits in, we can add some content to the government's empty policy debate and accelerate the process of decriminalizing encryption.

Conclusion: Electronic Privacy and Security Decisions Are Not Set in Stone

The Vanguard privacy and security conference was prepared as a follow-up to our earlier conference on electronic commerce. Its goal was to raise our sponsors' consciousness on the risks of life in Cyberspace and to provide state-of-the-art strategies for avoiding those risks. As a secondary goal, we hoped to remove Internet security from the world of mythology (and its stepsister, media hype) and bring it into the world of cold reality. For better or worse.

This paper began by comparing the development of Cyberspace to the construction of the masterpiece of suspension bridges, the Brooklyn Bridge of John Roebling, which has withstood 100 years of skepticism about its revolutionary design. Now is perhaps the time to say that that analogy was not entirely apt. The Brooklyn Bridge was rendered in concrete, stone and steel cable, and any limitations or weaknesses

in either design or implementation have become permanent fixtures. This is not so with the emerging world of public and private networks, which are by design virtual switches, capable of being largely invisible, and hence rebuilt in pieces or in whole as time goes on. It is not too late to reconsider the design decisions that have so far been made, and it will never be too late to make improvements.

That is both a virtue of the environment and a responsibility of its users.

Appendix: Who's Who

Those referenced in the paper who participated in the Vanguard conference, "Privacy and Security: Keys to the Electronic Trade Exchange," February 2-3, 1995:

David Bauer, *Principal, Morgan Stanley Company.* He is responsible for the definition and implementation of security for all of Morgan Stanley's computing and communications infrastructure.

William Cheswick, *Senior Researcher, AT&T Bell Laboratories.* Co-author of *Firewalls and Internet Security: Repelling the Wily Hacker*, he is Bell Lab's resident expert on computer security gateways.

Whitfield Diffie, *Distinguished Engineer, Sun Microsystems.* He is best known for his 1975 discovery of the concept of public key cryptography.

Raymond Kammer, *Deputy Director, National Institute of Standards and Technology.* He is responsible for the daily operation of NIST and for long-range planning and policy development.

Alan Kay, *Apple Fellow, Apple Computer.* One of the great pioneers of personal computing and considered a technology visionary, his current interests continue to revolve around creating better learning environments for children and adults using computers.

Steven Levy, *Author and Journalist.* Author of *Hackers, Artificial Life* and *Insanely Great*, and technology columnist for *Newsweek*, he is currently working on a book about cryptography.

Rober Lucky, *Vice President of Applied Research, Bellcore.* He is an internationally recognized expert, author and commentator on the state and future of data communications technology.

Nicholas Negroponte, *Professor and Director, MIT Media Laboratory.* He is one of the world's leading authorities on how computers are revolutionizing the delivery of information and entertainment services.

David Reed, *Senior Scientist, Interval Research Corporation.* An information architect, his research focuses on exploiting new technologies that help people and organizations function more productively.

Tsutomu Shimomura, *Senior Fellow, San Diego Supercomputer Center.* One of the country's top computer security experts, he made headline news in early 1995 when he tracked down the intruder who had invaded his computers.

Cliff Stoll, *Author.* Author of *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, he has firsthand experience as a computer security expert.

W. Scott Stornetta, *Co-Founder and Chairman, Surety Technologies Inc.* He co-invented an innovative digital time-stamping technology that locks the contents of electronic documents in time.

About CSC Vanguard

CSC Vanguard is a research and advisory service that helps its sponsors shape their future business strategies with an eye toward the emerging technologies that will affect them in the next three to seven years.

Membership in CSC Vanguard is limited to a select number of prestigious organizations worldwide. These organizations see technology-enabled business innovation as critical to their future success, and are aggressive with emerging technologies to realize compelling business opportunities. The sponsoring executives are the people most directly charged with bringing new information technologies to bear on business process and product change: chief technology officers, chief information officers, business strategists and other executives leading change. Membership is renewed annually and entitles the sponsoring executive to all scheduled events and deliverables. For more information, please contact Richard Schroth, executive director, at (617) 499-1526.

About CSC

In an era when the foundations of business structure and management are changing irrevocably, CSC offers a complete range of services to help client organizations respond to the demands of a new business world. CSC draws upon the pioneering research that led to CSC Index's ground-breaking concepts of business reengineering and the value disciplines approach to business strategy. By reinventing the ways they perform work and deliver value to customers, CSC clients achieve breakthrough improvements in business performance and competitiveness along the dimensions of cost, quality, speed, customer service and capital. In addition, CSC's expertise in all facets of information management helps clients achieve dramatic improvements through accelerated systems development, systems integration, I/T management consulting and information systems outsourcing.