openness
trust
sovereignty

Openness, Trust and Sovereignty

A Report of the 2004 Rueschlikon Conference on Information Policy

by Kenneth Cukier

The Rueschlikon Conferences
on Information Policy in the New Economy

in cooperation with

Swiss Re
Centre for Global Dialogue

To order additional copies of this report please contact:
Fritz Gutbrodt, *Head*
Swiss Re Centre for Global Dialogue
Gheistrasse 37
CH-8803 Rueschlikon
Switzerland

For all other inquiries, please contact:
Viktor Mayer-Schönberger, *Conference Co-Chair*
The John F. Kennedy School of Government
Harvard University
79 JFK Street
Cambridge, MA 02138
Email: Viktor_Mayer-Schoenberger@harvard.edu
Web address: http://www.rueschlikon-conference.net

Design: K. H. Machat, www.heikenz.net
Published in the United States of America in 2004

Contents

Appendix

Trust is essential to all economic activity. Surveys have shown that a perceived lack of it has particularly detrimental effects on the Internet economy. Trust is hard to build, and easy to lose. As trust turns into a central business imperative for the continuous development of the information economy, we need to better understand how to lower possible legal, economic and technical barriers to its implementation.

Openness and transparency is one strategy to build trust. Erecting barriers, and thus excluding others in order to reduce the likelihood of attacks that might violate trust, is another. There is an intense debate about which strategy is preferable - for distinct circumstances as well as in general terms. Furthering trust requires us to have a better sense of the relationship between trust and openness.

Shifts in trust, openness, and accountability enabled by the Internet – for business partners, market makers, and financial institutions shouldering the transactional risks – prompt us to think about liabilities and risk. When these issues are examined from the perspective of a global Internet economy in which concerns about Internet security have grown drastically and assertions of national sovereignty challenge the commitment to openness, the characterization of risks and the design of workable business models become even more complex and important to think through.

These issues were at the heart of the 2004 Rueschlikon Conference on Information Law and Policy. The conference is an annual gathering of a small group of select experts from around the globe. Its aim is to stimulate dialogue between business strategists, regulators and academics. Organized by Professors Lewis Branscomb and Viktor Mayer-Schönberger of the John F. Kennedy School of Government, Harvard University, in cooperation with Fritz Gutbrodt and the Swiss Re Centre for Global Dialogue, the 2004 conference took place at the Swiss Re Centre June 10 to 12, 2004. Forty-one participants debated for three days the salient issues of trust, openness and sovereignty. The following report provides a detailed summary of the discussions. In accordance with Rueschlikon Conference rules to ensure an open and lively exchange, the report refrains from attributing statements to individual participants.

We thank Kenneth Cukier, the author of this report, for so successfully weaving a common thread out of the three days of intense discussions.

Lewis M. Branscomb, *Aetna Professor of Public Policy and Corporate Management, Emeritus*
Viktor Mayer-Schönberger, *Associate Professor of Public Policy, Kennedy School of Government, Harvard University*
Fritz Gutbrodt, *Head of Swiss Re Centre for Global Dialogue*

August 2004

Report: Openness, Trust and Sovereignty

Executive Summary

To buy a book at a store, it's sufficient to reach into your wallet. Online, it entails much more: Might one's credit card details be spied as it travels along the open network? What if the store is unscrupulous and never sends the tome? And whose laws are upheld if the buyer and seller are in different countries? In short: Openness, trust, and sovereignty – the theme of Rueschlikon 2004.

In 2003, retail e-commerce was valued at $44 billion in America alone according to the US Dept. of Commerce, growing by over 25% annually. As more of our activities take place online, the risks and rewards surrounding openness, trust, and sovereignty deserve to be better understood. This overview summarizes the discussion at the fourth annual Rueschlikon conference, held June 10-12, 2004. Seven dominant themes emerged:

- **Trust Meets Technology** – Trust lowers transaction costs and is more efficient than institutional mechanisms to assure correct behavior. The Internet is ripe for abuse of confidence, yet technology can actually lower risks and increase trust.

- **Valuing Trust** – Trust is a valuable economic asset we really only appreciate when it is lost. Smart companies realize that there must be confidence in the system as a whole, not just the individual firm.

- **Virtual Worlds, Real Issues** – As online worlds where people interact go mainstream, trust becomes more important yet institutions like the law are not easily imposed. Regulations may need to be reinvented to adapt to the new environments.

- **Online Risks, Real and Hyped** – Some of the misgivings about the Internet are misplaced – be it the threat of hackers, corporations or even government. It's imperative to focus on the tangible, identifiable harms.

- **Multi-Model Approach** – No one system will be sufficient to foster trust on the Internet. Luckily, the Internet itself gives rise to experimentation, diversity and co-existence among different models.

- **The Nation vs. The Net –** Government regulations are still important – but they must be carefully initiated lest they harm the very thing they strive to protect.

- **Private Sector, Public Sphere** – Trust can occur in both closed and open situations – what's important is the right model fits the circumstance.

Looking ahead, attendees were surveyed on what Internet regulation might look like in 2015. The majority believed it would be an amalgam of national laws, international regulations and private-sector norms – not predominantly national rules or international accords. However, as trust is foremost a sociological phenomenon, the technical and legal tools will be severely challenged.

Taken together, the consensus among Rueschlikon 2004 attendees was there is an urgent need to foster trust without jeopardizing openness or innovation, and to minimize purely national rules in favor of a more comprehensive approach to policy-making. In this way, the risks associated with Internet activities may stay within tolerable limits. If this fails, however, participants believed the confidence in the network would erode, and people rely on it less than they otherwise might.

Delta Airlines, Barnes & Nobles and Sotheby's seem to be in radically different industries – air travel, book selling and auctioneering. One involves transport, another retail, and the third, a middleman with a respected platform for exchange. This much is obvious. But when one considers how these companies translate themselves online, something interesting happens. Suddenly, they and their virtual equivalents – companies like Travelocity, Amazon and eBay – don't seem so remote from one another. When they move into a virtual setting, the very nature of the business changes: it becomes foremost about trust.

Why should this be so? Of course all businesses, from airlines to auction houses, need to win the confidence of their customers or they go kaput. But on the Internet, this is magnified – and the consequences of a lack of trust more stark. There are three main reasons for this. First, the Internet is inherently untrustworthy – as an open network with decentralized control, it encourages brilliant innovations but also allows a certain degree of anonymity that enables things like spam and viruses. Second, the virtual setting lacks many of the social conventions of trust that we appreciate in the offline world (and sometimes take for granted), which need to be recreated in the technology. Third, the global nature of the medium creates jurisdictional uncertainty.

If e-commerce, today estimated at $5 trillion annually worldwide, is to continue to flourish, these three thorny issues – openness, trust, and sovereignty, the theme of Rueschlikon 2004 – must be addressed. After three days of discussions at the fourth annual Rueschlikon conference on information policy, held June 10-12, 2004, no answers were fully formed, but a number of broad patterns appeared. This conference report tries to present them in a coherent way, pointing out where consensus emerged and where thoughtful disagreements challenged our perspectives. As is Rueschlikon tradition, the discussion was on a strict not-for-attribution basis, to encourage frank dialogue.

This report is divided into a number of sections (whose headings will be familiar to conference participants, since they were inspired by the colorful turns-of-phrases from the discussions). First, the report surveys what trust is and its economic value. Then, it examines the issues of how trust works in a novel area, but a possible test case for society as it moves online: virtual worlds. From there, the report considers different problems related to trust online, and then different approaches to remedy those concerns. In so doing, it raises one of the central themes of the conference: the openness of the network. Finally, the report looks at the role of government to instill trust and regulate behavior, relative to non-governmental approaches by technological tools and the private sector.

A paradox inherent to the discussions is that participants considered how technology has changed the nature of openness, trust and sovereignty, while at the same time technology is not static but itself changing in ways we are unable to foresee.

This provided the backdrop for the most dominant aspect of the discussions: humility.

Trust But Verify

Can trust exist without mistrust? How we define trust determines what role we see it playing in society – and the role of technology in undermining it, or encouraging it.

As president, Ronald Reagan explained his approach to an arms limitation treaty with the Soviet Union by way of the Russian proverb "doveryai no proveryai" – trust but verify. This notion, more than anything else, served as the leitmotif of Rueschlikon 2004, and was evoked by numerous participants throughout the three days. However, there was no shortage of interpretations as to what it meant. For example, does it really mean "don't trust"? Does the need for verification require an independent authority – into which we must place our trust? To what degree is suspicion healthy versus self-defeating?

Participants offered a number of definitions of trust (though it sometimes revealed more about their professional perspectives than the term itself). A few definitions:

> "Trust means the invisible, but relied upon, presence of safety."
>
> "Trust is one party's confidence that the other party in an exchange relationship will not exploit its vulnerabilities."
>
> "Trust is the expectation of behavior based on experience – experience in both micro sense of economic activity, and cultural sense, as a broad web of shared experiences."
>
> "Trust is the social capacity to live with risk. … Trust itself is scalable, from paranoia on one side to overconfidence on the other."
>
> "Trust is like the reverse of public-key encryption: there is little effort to encrypt and large effort to decrypt. Trust is the other way around: it takes a large effort to build and little effort to unbuild (i.e. destroy)."
>
> "Trust is a noble but backward form of dealing with risk."

The diversity of views quickly made clear that no single definition of trust would be established – that like the Supreme Court's definition of pornography, we know it when we see it. Perhaps more importantly, we really recognize it only when we don't have it. As such, many descriptions of trust focused on what trust was not, or the characteristics of trust rather than trust itself.

For instance, some believed that trust is most important when there is no alternative to substitute for trust to reduce risk. Furthermore, one person boldly claimed that trust is not the natural state of things – that it is a Hobbesian world where people compete for scarce resources, and so to civilize the interactions we impose institutions like the law that is founded on this artificial trust. Another person submitted that trust is a way to simplify the complexities of life, by giving a zero probability to things that that entail risk, such as flying in a plane or putting money in a bank.

That technology erodes traditional trust is nothing new. The postal system brought mail fraud; the telephone gave rise to anonymous heavy-breathers; print and television media ushered in truth-in-advertising laws. So too, the Web engenders new crimes – which will be met with new solutions.

This cat-and-mouse aspect of technology – that it giveth as much as taketh away – was acknowledged to be a recurring historical theme. In Victorian England, for instance, railroad station "boosting" was a common crime, where teams would go from station to station exploiting the commotion of passengers getting on and off the train to pick pockets. That practice ended once the telegraph was introduced, and station chiefs at one stop could alert his counterparts farther down the line. The moral: "Technology enables new crimes, but also eliminates some old crimes."

One participant explained common components of trust and distrust. Considering them as antonyms was a helpful way to understand the issue. An excerpt follows:

Bases of trust:	**Sources of distrust:**
Common accountability	Asymmetry of information
Reciprocity	Short time horizon
Reputation	Anonymity
Third party guarantee	Lack of persistency
Shared norms	Uncertainty

Importantly, no one sought to revert to some illusory golden age of trust. Moreover, there was a provocative perspective that the lack of trust on the Internet might be taken as a sign of the maturity of the medium. What became clear is that as problems have emerged over time, intermediaries have cropped up to mitigate risk – be it laws, currencies, navies, banks, insurance companies – or PayPal, eBay reputations and Amazon reviews.

Ultimately, it was agreed that trust is foremost a perception. The illusion of trust can be as powerful as actual trust (akin to Peter Pan's Tinkerbell, who only exists if you believe in her). Yet this, too, begs questions: For instance, paper money is as real a store of value as digital bits – do we give preference to one and less so, the other? Why? And for how long will this be, as we race into a world where more of our life takes place through a keyboard and screen?

As Reagan's Russian proverb suggested, trust is tied with verification. Yet verification has a cost. For things where the consequences of abused trust is low, verification doesn't make sense, say, whether a newspaper boy will really hand over the broadsheet when I toss him a nickel. Not so where the consequences are high, such as, handing over retirement savings to a stock brokerage. This creates a conundrum. As one participant noted: "Trust not just experiential but reputational. Most people don't have time to experience it before having to trust it."

Is Chevrolet as Trustworthy as Your Mother?

Trust has an important economic value. But what is the rapport between specific trust (in a person or an institution) versus systematic trust (in a system or a society)?

There are many reasons to buy a car: safety, fuel economy, price and of course, speed and a chic design. So it might be odd for an automaker to pitch a product without any vehicles in the advertisement – instead, a photo of a mother holding a smiling child. But such is the case with "Chevy's Genuine Customer Care" ads. What they are selling is dependability; the economic asset is trust.

As one person pointed out, honesty can be treated as a public good. "Trustworthiness," he said, is "not just a marketing convenience." Yet it raises a classic collective action problem: to what degree does the incentives of any one player coincide with the interests in the system as a whole? Or, by trying to instill trust in a particular product, might trust in the market itself be destroyed?

Some industries understand this better than others. For instance, there has long been an unwritten agreement among airlines not to advertise based on safety, for obvious reasons. Likewise, as a start-up company Amazon.com had a formal media policy that it would never comment on Internet security issues (unless to defend itself in the press). Rueschlikon attendees heard the situation of ISPs in Japan, who saw their subscriber numbers drop and stock price sink due to privacy violations that damaged consumer trust in the industry as a whole.

On a purely economic level, data suggests that trust lowers transaction costs. According to a study of procurement productivity across auto makers, companies with greater trustworthiness among suppliers and business partners had far lower transaction costs. For instance, Toyota's trustworthiness rating is twice as high as GM's; the payoff is that the Japanese auto company's procurement productivity is seven times higher than the American firm's. This pattern, where low trust begets higher transaction costs, repeated itself for the five car makers studied (source: J. Dyer, “The Role of Trustworthiness in Reducing Transaction Costs and Improving Performance”).

Technology, it was noted, allows new ways to build trust. In the case of carmakers, the mechanisms of trust that suppliers place in Japanese auto firms allows the companies to purchase their parts at a slightly lower cost than US firms – over time, the aggregated savings is substantial, and makes Japanese carmakers more price competitive. (That said, one respectful criticism of the example was that Japan’s banks have also placed a high degree of trust in the companies with whom they provide loans, and for that, their record is less rosy than the automotive firms’.)

Surely transaction costs are decreasing over time, and with the Internet able to grease the wheels of commerce, it is falling further…? That common perception turns out to be untrue. Transaction costs have actually increased as a percentage of non-governmental gross national product in the US, from 24% in 1870, to 52% in 1940, to 65% in 2000. Transaction costs, in this measure, are the expense related to things like searching for a transaction partner, negotiation, monitoring and enforcement that would not be incurred if one were trading with oneself. Clearly, the Internet has decreased some types of transactions costs (for instance, the cost of communications) but actually increased others (such as the cost of attaining trust).

Providing trust doesn’t come cheap. Among the mechanisms to enable trust, three were singled out: contracts, repeated interactions and reputation systems. Contracts are costly to write and costly to enforce. What’s more, they rely on a common infrastructure (such as a court system) that has to paid for by someone. The second approach, repeated interactions, also extracts a cost, since one loses the benefits from spontaneous trade as well as comparative advantage, specialization and new entrants into the market. Reputational systems bear a cost in another way: the time it takes to develop good standing.

A concern is that the value of trust is different for participants, as the notion of collective action dilemmas suggest. Here, the distinction was made between systemic mistrust and mistrust of individual things, that is, the bank fails, versus the banking system failed. Online businesses are taking it seriously. For instance, according to one participant, there are100 people at a division at eBay who develop metrics on how much transactions increase if trust increases. It’s only logical, considering that there are more people with PayPal accounts than AmEx cards.

Ultimately, the most important value placed on trust comes when it is lost – when we ruin the worth that we would have otherwise have had if trust existed. This is tougher to measure. But there is clearly a huge economic dimension to this. Might the accounting scandals that rocked US companies in the past four years (Enron, WorldCom, Delphi, Tyco, etc.) have spooked investors to putting less assets into equities? Many people believe so, as money taken out of the stock market was placed into more tangible assets, that is, real estate. If Americans are less likely to put their money into stocks, this affects the availability of capital for US companies. It shows the degree to which trust in the particular affects trust in the system, and vice versa. Trust has a huge economic worth.

Homo Ex Machina

One novel aspect of the networked society – virtual worlds – may serve as a petri dish for how to develop new mechanisms for trust, openness and (gasp!) sovereignty, too.

"Every civilization begins as a theocracy and ends as a democracy," wrote Victor Hugo. The 19th century French writer would have been impressed with the microcosmic societies cropping up online, where users have begun to supplant the companies that constructed the environment as the sovereigns. In one world, the Sims Online, a shadow government formed that started, ironically, as a mafia. Online worlds began in 1978 as text-only environments. Today, the growth of these distributed network worlds exceeds the growth of the Internet itself.

Why should we care what a bunch of oddball teens do? For a number of reason, first among them that the demographic is more adult Main Street than Sesame Street. Moreover, there is real money involved, and it is growing. Total eBay sales of virtual items in the first quarter of 2004 reached $5.85 million, and the amount is doubling annually. Acres of virtual real estate have real-world market values. One game in Iceland lets users put in and take out money – a potential source of money laundering. Still, this misses a bigger point. The policy issues with which these environments must contend seem to be an early predictor of how trust mechanisms can be established online, as well as potential new approaches to sovereign authority.

"Online worlds offer a significant challenge to the infrastructure of the modern nation-state," noted one participant. This is due to the way it strives to define property as well as treat privacy law, intellectual property issues, electronic currency, online identity and citizens' rights. "It will be the video game industry that deals with identification, not governments, though this makes governments queasy," the person said.

As a result, a lot of experimentation over policies is taking place. Consider intellectual property. In the virtual world Second Life, all intellectual property resorts to the user who brought the creative work into the world. Not so Sony Online Entertainment, where the exact opposite is the case; the company owns everything. Things get murky quickly: What happens when a user makes a replica of a Picasso painting for his digital domicile? Can the late artist's estate sue or demand a licensing fee? And what if a user in a virtual world starts a radio station and opens a music hall where online bands do cover songs by real-world acts? The recording industry around the world has tightly defined rules and revenue-sharing agreements for performances – online worlds throw it all up into the air, like Alice's playing cards in Wonderland.

The role of the state in these environments is ambiguous – for now. For instance, where online worlds are comprised of distributed servers spread across a score of countries, can virtual environments declare themselves sovereign? Microsoft's "click-wrap" end-user license agreements are considered contractually valid in most jurisdictions; can virtual worlds impose the same private-sector regulatory approach on its users, via contract law? Or does that constitute a return to lawless dictatorships of which people have spent millennia freeing themselves in the real world? No one went so far as to claim that online worlds constitute a rewriting of the social contract for cyberspace, yet the question, and fears, were considered. As one person explained: an estimated $100 million worth of transactions take place in these spaces – are taxes being paid? Who would collect them? Why?

The most important aspects of virtual worlds in the context of trust is that the confidence that users place in the environment doesn't pre-exist; it has to be created from scratch. "It's not 'slay the dragon' but medical records that will be stored on this – and what is the role of government and regulation then?" a participant asked rhetorically. Secondly, the trust that can be established in this environment may in some contexts exceed what exists offline. For example, a highly reputable person in a virtual world might be a college freshman with no credit rating in the real world. Clearly, we are present at the creation: what kind of changes do we, the deities, wish to make?

When Your Dog Sees You Naked

Everyone is nervous about online risks, from privacy to pornography to phishing. The state can surveill us and hackers track us. But might our mistrust be overblown?

When the debate over the European Union's privacy directive caused tensions between the US and Europe in 1998, the reason seemed to stem from basic ideological differences: Europeans trusted the state and feared privacy invasions by business, while the Americans feared governmental nosiness and tolerated intrusions from the commercial sector. This (admitted) generalization underscores the degree to which trust and risk tolerance differs among people and across cultures.

Likewise, at Rueschlikon, the skepticism that all potential online vulnerabilities should necessarily translate into real harms was colorfully expressed by one participant when the topic turned to gmail, Google's email service that triggers advertisements related to the content: "Worrying about your computer scanning your e-mail is like worrying about your dog seeing you naked." Perhaps. While every technology has real harms and hyped threats, a critical point is that it's not always possible to predict one day what will be of concern the next.

What is certain is that the openness of the Internet is being challenged in two fundamental ways; from its decentralization that is exploited by bad actors, such as spammers, and from a degree of centralization imposed by government and business to remedy those abuses. "Today, most people see transparency and openness as a peril, not a virtue," remarked one attendee.

The potential for a lack of trust in the network doesn't only come from bad apples at the edge, but the guardians at the network's core. The center holds – and knows. Indeed, a number of technologies and policies make this new centralization possible, which participants discussed in detail. For instance, network monitoring is commonplace. Software exists that triggers an alarm if a person has downloaded or uploaded 300 songs in a 24-hour period, to alert network administrators that the user is potentially in violation of copyright. The software is understandably popular with universities, which fear lawsuits by the Recording Industry Association of America over music piracy.

Moreover, there is another form of network monitoring to determine if things are amiss: software scans the traffic pattern on networks and builds a profile, so that it can detect a problem the instant it arises, such as a distributed denial of service attack. "It's like a beat cop," one person noted. "That's how we brought civility to society. It's not highly sophisticated and not treating everyone as a criminal – it's just watching," he said.

In the US, Internet service providers need to keep the DHCP logs (which indicates the Internet Protocol address people use through their ISP) for six weeks and possibly more. Internet service providers in Britain are required to retain all instant messaging communications for a full week. European Union retention rules on telecom traffic information are implemented inconsistently in national laws, and vary from a few weeks up to 12 months. Meanwhile, the mobile phone industry's geo-location services track users around the clock. Microsoft's personal identity service, called Passport, is a way to ease the process of divulging personal information to different Web sites, but whose very name smacks of vying to be a substitute for the state, which traditionally manages citizen's identify.

The line between the innocuous and the treacherous was examined during a discussion on email and spam. Although some participants initially questioned why a conference on the theme of openness, trust and sovereignty would end up talking so much about spam, other attendees rushed to point out that spam is representative of a plethora of online problems – that the open architecture of the Net allows and that governments can't control – which erodes the trust in the network. "The importance of spam is that it's a particular trust issue – trust in the functioning of the network. … Are we faced with a market failure in this sector? That's what an economist would normally ask, and then discuss those causes of market failure," said one person.

Spam is the most devious of online menaces, since it constitutes the openness of the network turned against itself. Email, generally speaking, cannot be trusted for three reasons: The sender's identity is dubious; the economics of sending email shifts the cost from sender to receiver which allows it to be used for a sort of "broadcast" model; and any message may be carrying a dangerous payload like a virus. How can we create trust in the architecture of the network? One model is to view trust in hierarchical terms. The first level is accreditation and second, authentication. This indicates and confirms online identity. Level three is reputation, the history of online behavior. Level four is enforcement, which includes a process to revoke the credentials.

Attendees built upon the model to note that trust is a relationship, which has an evolution. In a commercial sense, in the words of one participant, "customers are dating brands" but what they don't want are "one-night stands." The hierarchical model raised a number of questions. For instance, will we end up with a collection of "gated communities" or can the "frontier" ethos of the Net endure – that is, will we sacrifice innovation for order? Does the gated community model even scale to any meaningful extent? Secondly, will we still be able to have anonymity online; should we?

The issue of spam lies at the heart of the direction that the network seems to be headed – towards a closing of the Internet. When calling from a phone, or surfing Web sites, we take for granted that the number or address brings us to the right place; with email, we have been so accustomed to spam ruses, be it Viagra or viruses, that we treat messages with presumptive distrust. Few other things in society force consumers to interact with total suspicion; even advertising has consumer protection laws behind it. In economic terms (which one attendee implored we consider, cited above), the central issue facing spam is how to manage the opportunity cost of decreased trust in the network as a whole. As such, the acquisition costs in this context is building trust, and the retention costs are maintaining trust.

Ultimately, while some online threats may be overstated, they can still represent serious concerns. That is to say, just because we may not care if our dog sees us naked, it doesn't mean there aren't other prying eyes at the same time that might make us wary being nude. There was a consensus among attendees that it is important to specify what class of threats we are considering when we say we want trust or security. As an example of this, one participant explained that as banks invested in security, they reached a point where they didn't want more – it was too costly. They had accepted a level of 2% to 3% of problems. It wasn't a threat to the bank, other than an acceptable loss of money; the trust issue was brought to a tolerable level.

Perception is the critical component. For instance, we feel more secure (and the merchant fees are less) when we use a credit card in the real world than online, when in reality, the technology actually makes card transactions more secure online than when we hand it over to a waiter. Perception also changes the way we view threats.

As one participant noted about the discussions: “It’s interesting that privacy has not featured higher in trust as a concern. Is it possibly a result of Sept. 11, that it is not considered patriotic to talk of it? Or is there now a willingness to sacrifice it?”

Polytheism Is the Best Insurance

There is no single model to build trust online, and the Internet itself gives rise to different approaches. Experimentation, diversity and co-existence is in order.

To understand the degree to which the world today is different than the past, consider one participant’s experience traveling. The person was in Guatemala and ran into a bit of trouble. It presented a dilemma. “Do I call the American embassy or do I call American Express?,” the person wondered. “Instinctively, I knew,” the person explained, “AmEx – they’ll be sure to help me.”

The anecdote underscores the degree to which private sector based entities are assuming responsibilities that government once took on – and how we’re also willing to defer to them. In fact, in some instances, we actually trust them to help us more than government institutions; for instance, they may be faster or more efficient. So too with online trust, a number of models have emerged that ape traditional institutions in a virtual setting.

This section examines the breadth of ideas discussed on how to instill trust. It first looks at decentralized and Internet community-based systems. Then, it considers offline mechanisms, such as credit cards and the judicial system. Finally, it examines ideas on how to instill trust by imposing a degree of centralization on the architecture – through ISPs, as well as novel proposals to use the domain name system and the Universal Postal Union.

Decentralized, Internet-based systems have been fairly successful in establishing trust through a variety of methods. Some sites use transactional histories to build reputations, like Amazon or eBay. Others, like social networking systems, leverage existing trust relationships by mapping them online. A third dimension is community status, such as with the open source community, blogs and the ranking of comments on the celebrated techie Web site Slashdot. A fourth approach is establishing trust through transparency and process, as SquareTrade does.

In the case of transactional and reputational systems, eBay and PayPal have generated trust in a number of ways. It easily integrates the system directly in the transaction engine, so it’s simple. Also, it gives verification to both parties so they can control the money flow. Finally, because eBay’s transactions entail less risk when PayPal is used, the auction company can offer insurance on transactions, which increases user trust. The result is that 70% of eBay’s volume in the US uses PayPal (which also helps explain why eBay bought the company in 2002).

One limitation to the eBay and PayPal model is that it does not work for services, but for mainly high volume, relatively low value transactions. In the area of social networking applications, the LinkedIn model is designed for services or work transactions. The premise is that friends-of-friends are reliable and that reputation is what qualified people with experience with your work say about you. In LinkedIn, people publicize their number of connections and number of endorsers. This allows users to identify shared connections, and if so, by how many degrees of separation. The system takes care of the issue of identity as well as enforcement, by staking so much on a publicly transparent reputation system.

Yet some of the less mechanistic and subtler things account for LinkedIn's success. For example, the design interface is honed so it is easy for people to understand, simple to use and reliable. LinkedIn has a "five-second rule" which says that if a customer doesn't understand the system in that length of time, they won't use it. "The rule on consumer, mass-market applications: any complexity means near zero adoption," one person said.

So much for bringing parties together – what happens when disputes arise? That area is the domain of SquareTrade, It provides a trust seal to merchants that is transparent in the protections afforded to buyers. The company uses that as the bases for an online dispute resolution mechanism that is suited for the virtual environment, where transaction values may be lower, across different national jurisdictions, and the need for quick, low-cost mediation paramount. Providing this sort of transparency and assurance leads to greater confidence in online transactions.

While the online world has developed a rich array of trust institutions and processes, a number of offline mechanisms were considered (though not always well received). The most obvious mechanism for offline trust today is the credit card system. It allows buyers and sellers to pay with plastic, based only on trust that the transaction will be honored. The reasons it is so successful was closely considered for the lessons it offers.

First, the $50 limited liability that is often held up for praise was not instituted by design. Initially, the credit companies sent out unsolicited cards, which were stolen and used. This became so prevalent that the federal government stepped in and required limited liability – which at first the card companies hated, but later learned to love. Second, the credit card system shifts costs from the consumer and the bank to the merchant. The seller pays a fraction of the transaction cost to the bank. More importantly, the merchant has to bear the cost of validating who it transacts with, and assumes the liability if it fails to do so. The principle that authentication for transactions has been outsourced to the payment industry is one of the most germane aspects of e-commerce going forward, and an important trend as other trust mechanisms are considered.

The social consequences of the primacy of plastic are mixed: in the West, and among the wealthy, where credit cards are the norm, this system poses no problem. But among the poor, the lack of a credit card may exclude them from many transactions. In places where credit cards are not prevalent, such as in Asia where mobile phones are sometimes used as payment methods, other systems will need to emerge for trustworthy e-commerce to flourish. Meanwhile, even in the West, mobile phone companies are vying to take on greater roles, such as acting as banks. This is ironic, given that their telecom peers, Internet service providers, are doing all they can to limit their liability, not increase it (an issue that is dealt with later in this section). As the two types of networks merge, it is unclear where they will end up in this regard.

Another classic method to deal with trust, that may offer lessons to the online world, is how the judicial system operates. By the time the parties enter into court, it not only represents a breakdown of the system of trust, but also its hallmark. The legal system provides rules that are generally transparent and predictable. For liability matters, the principle is usually that is falls upon the least-cost avoider. That is, the party who can correct the problem easiest is where responsibility is placed. And if the party has followed a recognized "due care" standard, then it can escape liability if something goes awry.

Yet there is a major shortcoming to this system, as it operates in practice. There may be bad laws, by precedents, and (alas) bad lawyers – or for cyber-esquires: "spambulance chasers." As one participant explained eloquently: "Courts are not benign, beneficent institutions that operate in the abstract. The legal system is driven today by the profit motive, particularly for liability issues. But the courts are a very poor system for adjudicating these kinds of problems." For instance, they are not active where there is no aggrieved party or potential financial opportunity. "Where there is a profit to be made, it becomes a center for abuse. In the case of data protection, it relies on adherence to regulation itself, not its enforcement," since by that time, the damage has already been done.

As the liability question rears its head, one obvious place for many of the trust mechanisms to be instituted is in the heart of the network itself, as it is handled with the telephone system. Are the network operators up for the task? Can they be trusted themselves? The basic dichotomy in telecom regulatory policy is between carriage and content. Networks focused on the former and avoided the latter, in return for immunity from being held accountable for what they transport.

When ISPs emerged, they sought, and generally got, the same legal distinctions. However, taking on the responsibility of building trust mechanisms into the infrastructure seems to fly counter to this. It also does something very un-Internet-like: it centralizes the architecture, rather than retains the decentralized character of the network, which is credited with the Net's capacity for unfettered innovation. Network operators say they don't want the responsibility of overseeing trust online – from fingering file-sharers to policing pornographers – and many people are wary of giving them that power. But ISPs already take on some roles; BT has instituted a white list for its users to reduce spam, and AOL actively blocks the Web addresses that are sent inside spam to AOL customers.

The reason for the persistence in considering network operators as the place to impose mechanisms to achieve trust is because it's efficient: A small number of companies control a large amount of traffic. These ISPs already make decisions on what people see and do online, and how the network works, though not always in ways that are apparent to general users. Unsurprisingly, it's the network operators, like MSN, AOL and Earthlink that are taking the most active and effective steps in curbing spam, where companies at the edge of the network are inherently less effective.

The main problem with giving the ISP this control is that they may take more extreme measures to protect themselves than the law itself requires. As an example, one participant explained an informal study by the Oxford Internet Institute to gauge how ISPs in Europe and America comply with take-down requests of purported copyrighted material. They posted online, with irony, John Stuart Mill's essay "On Liberty," which is in the public domain since copyright has long expired. They then sent a take-down requests to an ISP in both regions. The American ISP acknowledged the letter, did not remove the content, and asked for more information; the European ISP took down the content no-questions-asked – even though the text is perfectly legal.

Finally, attendees considered two proposals to increase trust by bolting public policy goals onto the technology. The first idea is to require that all Web addresses refer to a specific territory; global top-level domains, such as .com, .net, .org, would be made pointers only, and tied to a sovereign entity. This would eliminate the jurisdictional quandary that occasionally happens today, and would be the first step to imposing formal identification rules on an Internet presence. The second proposal was to invite the Universal Postal Union to do for email what it has done since 1874 for its paper-based ancestor. In the digital world, the UPU could enable electronic postmarks in the 190 countries that are members, set international rules for them and prosecute violations.

Attendees were lukewarm on the proposals. Though fascinating as thought-experiments, many people felt that Internet addressing issues were messy enough that to impose more regulation might encumber the Net rather than solve its problems. As for the UPU, some attendees believed that an intergovernmental agency overseeing the Internet would likely bring the pace of technical innovation down to the speed of a post office clerk and third-class mail.

The issue of regulating at the center versus at the edge served as the backdrop of the discussion. For example, one participant criticized ideas such as a global identification hierarchy at the packet-level, a sort of "license plate" for packets, because it would break the end-to-end structure of the network. Doing it at the edge, not via the ISP at the core, might be better to preserve the Net's openness to experimentation and evolution. As another person chimed: “We put innovation above all other gods” – a fitting aphorism when being ecumenical about approaches to trust.

Among the diversity of approaches that are possible, one important aspect is that interactions can still occur when there is little trust – in fact, it can be designed into the relationship that way. The Sept. 11 hijackers were a virtual organization and their activities would have been almost impossible to do in the days before the Internet. Yet their model of interrelationship is the inverse of eBay – there is little trust among al Qaeda cells. Rather than an interconnected network, it is a disconnected network, yet it still interacts. Though an unpleasant example to consider, it nevertheless suggests that there are many models and levels of trust and openness.

The End of Virtual Reality

The Internet is a unique place where territorial rules don’t apply – or so some thought. Then we all grew up, and realized governments have a role. But what role is best?

In the final negotiations of the creation of the World Trade Organization in 1994, the French government won a “cultural exception,” which suggested that artistic works were somehow special, and shouldn’t be treated the same as other merchandise or commodities. Four years later, the US government would go to the WTO and argue for an “Internet exception.” It didn’t call it that – the policy was referred to as a “tax-free Internet,” prohibiting tariffs on goods sold electronically – but it amounted to the same thing. The anti-regulatory ethos concerning the Internet that dominated the 1990s is founded on the same principle, that the Internet is inherently special, and needs to be free of offline interferences in order to best develop.

No serious observer of technology policy really believes this anymore, if they ever did. The real debate is over where the balance is struck. Indeed, the most spirited discussion at Rueschlikon was over this issue. Without rehashing old clichés, it truly did divide many (though not all) of the European and American attendees, the former taking a more favorable view of government action, while the latter less so. The irony is that the US government funded and oversaw the Net’s initial development (albeit in a very hands-off manner), and the US-inspired metaphor for the network, the information highway, implicitly evokes the idea of rules of the road in order to make travel and transport possible. As the Net becomes mainstream, it must provide the same assurances that other critical infrastructures do. And that, some participants argued, is a responsibility of the state, not something that can be left to vacuous catchwords like “industry self-regulation” and “marketplace solutions.”

In the words of one participant: “The Internet isn’t virtual reality anymore – it is reality. It effects everything on the planet, something that we don’t even grasp ourselves. The idea that the Internet is outside government power is a simplistic view. We can be creative in the way we have government deal with the Internet, but we can't believe that government should be below it. … We are dealing with very sensitive issues, philosophical and cultural issues, inside every country, and [governments] are not willing to let go without a fight. This may seem to contradict the nature of the borderless network – there *are* borders in cyberspace," he said, the final phrase intentionally borrowed from the name of a classic 1997 book edited under the auspices of Harvard's Information Infrastructure Project.

Governments, the person continued, "need to create a sense of people believing in the network they're living with, that the network is not superimposed on them and the very essence of their lives. If we're not able to make people feel more strong and secure in the architecture of the information society, we have a problem that is more important and not just about technology, but about the world we're living in. We don't have to imagine that the network is separate from our lives and laws – we have to build an architecture [for that]. … Do we need to change the core principles of the Internet? I don't think so. We can have smart regulations."

Some participants took issue with the call for more assertive government influence over the Internet. "It turns every country into China," said one person, referring to the difficulty in distinguishing among censorship by states. Another attendee questioned why, if there is a global Internet address space and users are free to chose among the myriad content, that government should have a problem letting citizens choose the cultural experience and norms they wish on the network. A compromise, he cracked, would be to flash a warning label atop Web sites like those found at movies or on cigarette packs: "Warning: You Are Leaving Your Cultural Expectations!"

However, the sentiment that government needs to do more to ensure trust online was echoed by many other participants during the discussions, in private conversations, and in break-out sessions. The most remarkable thing about the view is the seeming need to express it in cautious, hushed tones, as if it is so contrary to the dogma of the day that it is akin to defending czarism.

Another participant emphasized the symbiosis between the public and private sectors. For instance, the person noted, "government generates and underwrites money as the basic trust infrastructure for commercial exchange," but "the private sector guarantees payment, collection structures, global operations of credit card companies and risk insurance." Likewise, he asked: "Can trust be privatized"? This would entail things like data protection and privacy, consumer protection and secure, reliable financial transactions.

A sort of compromise position was examined, when a person pointed out that there was natural room for co-existence. An 80-20 rule applies, he said, concerning dispute resolution mechanisms. "The private sector can solve 80% of the problems and for the remaining 20%, we need government to step in."

While the private sector could, and sometimes does, manage many of these functions, the concern of government regulators is that market power works often by monopoly structures, and distribution structures in e-commerce are usually dominated by network effects. As one attendee said: "We will have trust, the problem is who controls it, and because of network effects, whether it will be controlled by very few companies."

This underscores an essential dilemma. The myth of the Internet holds that the technology inherently democratizes the market for e-commerce, creating more buyers and sellers and enabling more transactions among them. But what if this is false? There is a body of scholarship that suggest the Net's most sacrosanct assumptions must be reconsidered. Instead of a transactional and informational utopia where everyone interacts with one another, the Web is characterized by so-called "power laws," that is, winner-take-all patterns that actually concentrate online activity. Thus, we rarely buy books from corner booksellers on the information highway; we use Amazon. We don't survey yard sales on the front lawn of cyberspace; we go to eBay.

This view suggests that because trust requires a degree of vulnerability, users may end up limiting the number of partners they agree to trust, thus narrowing the field of entities with whom they transact. On one level, this has already happened and will continue. Yet it is not the whole story. While the Net lets the big to get bigger and winnows the breadth of parties we interact with, it is more likely that people will still want the possibility for direct interactions that bypass the large sites, in the same way that the advent of radio obviously didn't mean the end of the telephone.

In this respect, the Internet doesn't seem very different than the offline world, where we groan about mega-stores like Wal-Mart growing ever larger, yet continue to purchase chic threads from boutique clothing stores in Soho. Indeed, what may crop up are trust-intermediaries that assuage our concerns, akin to how credit card companies free us from fretting about buying goods in a foreign country – a trend that is considered in the final section.

Regulation is Perversion

Public policy is only one of many levers to instill trust, manage openness and uphold some sort of sovereignty on the Internet. Sometimes it is not the best one, either.

"Oh my God! The ITU with guns and badges!," said one participant, humorously melding two earlier slides, one referring to the International Telecommunication Union and the other about sources of authority. "Gods and market forces – governments don't trust either one," said another person. And upon hearing the "bumper sticker" insight that "regulation is perversion," a third attendee quipped devilishly: "That must be why I like it so much!"

Government regulation was the Banquo's ghost of Rueschlikon 2004, occasionally floating through the walls, taking a seat at the table and striking terror in those who saw it. There was a sentiment, although not universally shared, that public policy inherently introduces a foreign intermediary into the innards of the Internet which harms its decentralized model. Moreover, there was a concern that regulation risked giving rise to unintended consequences that could be harmful to the Net. "Rules are mirrored," one participant said. "They may be reversed, distorted – they are mirroring rather than transferring directly."

One person suggested that to understand why the Internet can be governed differently than other communications technologies, it was necessary to understand how they were organized in the past. Consider "mail governance": citizens were at the bottom, hundreds of government's post offices above them, and the Universal Postal Union at the top of the pyramid. "Phone governance" also takes the shape of a pyramid, with rate-payers at the bottom, state-run telcos higher up, governments above them, and the ITU at the top.

As for the Internet, the entire pyramid is placed on its side, the person suggested, and instead of a hierarchy, the governance is shared alongside each other. There are millions of Internet users making free choices over software, hardware and services. Alongside that are thousands of technology companies and Internet service providers independently vying for customers (albeit almost no competition in mass market software). Smaller in number – and seemingly less influential – are governments and national private consortia working on Internet issues. And then, far in the corner of the base of the pyramid are a few intergovernmental organizations, standards bodies, and international NGOs. The implication was that the Internet's decentralization offers more freedom for consumers, eliminating the traditional top-down structures.

The characterization of Internet governance generated strong controversy. It seemed to some attendees an idealized and self-serving portrait of how the Internet works, purely for the purpose of keeping government away.

"What's the point?," asked one participant. "This is what we want," the person presenting the model said. The room instantly became abuzz as many attendees, particularly from Europe, scolded "that's what *you* want!" One person parried: "This is a political statement – libertarianism – not an economic one. This discussion is not about creating a revolution in the way we regulate things. Why not push for that approach for offline issues, too?" The person's defense: "This is the way the Net has run." Another repartee: "This is the way the wild west is run, too!"

"This pyramid is a utopia," said an attendee, as the room quieted down. With hundreds of millions of Internet users, and the Net effecting all people everywhere with real implications, it is unrealistic to govern it as a Swiss canton, he said.

Just as in the 1930s when trans-Atlantic planes would land on a foreign airstrip unannounced and governments realized they had to do something, so too, it was said, governments need to act now.

"We disagree," said the model's author. Another participant offered an olive branch: "Are we talking about consumer sovereignty based on perfect information? Can we square the circle?," he asked. "We can agree that increased information for consumers is a good thing," was the ultimate terms of the verbal cease-fire.

The lively debate highlighted the differences in attitude concerning public policy. To what degree government should impose constraints on Internet users is made a more difficult question because so many of the issues confronting public authorities are new. "Is trust online like whether to use seatbelts – should you be forced to use it [so you are protected]?", one attendee asked. "Or is the individual users like Typhoid Mary," and a failure to adhere to safe Internet practices doesn't just hurt you but may dangerously infect others?

Others viewed government as a recourse if something goes wrong. For instance, the EU data protection act provides European citizens with confidence that if one suspects a problem, there is something they can do about it. To be sure, the empirical reality is less rosy – for instance, in Germany, which has the strictest privacy laws, there has not been a single court case to test them. Still, that represents the concrete aspect of trust, when much of trust is less tangible; just having a sense of reassurance establishes trust itself.

In promoting the role of the private sector to instill trust rather than government, another attendee sought to extend the Internet-to-road metaphor, which is typically used to argue in favor of government action (as it was at the start of this section). "FedEx does not go to the government and ask for roads so that customers have trust. Governments make sure there are roads – and then it's up to the users to build trust," a participant said. The analogy is imperfect – governments also ensure road signs, highway patrols and traffic courts. But the broader point, that users define the character of the infrastructure, still stands.

The central question is whether there is a threshold where government action is necessary. What is required is that users have an aggregate sense of comfort in their surroundings. That said, a high level of lack of confidence and trust leads to a constant skepticism of technologies, a situation like in the Soviet Union, where there was pervasive mistrust of institutions. This would hold back online development. As one participant noted: "People don't want a New Economy, but the old economy more convenient."

Indeed, despite the complaints about how countries impose laws on the global medium, the current approach of national regulation actually resembles the architecture of Internet itself: it is decentralized and distributed. On the Net, power rests at the end-points; in international policy, the same still holds true. Governments, akin to nodes at the edge, set their own course; this effects their own citizens but rarely interferes with the rest of the interconnected network of nations. It is not as bad as many of the possible alternatives, such as top-down control from the core. One person referred to it as “the network of filtered networks”; a way to preserve “a necessary chaos” amid governmental regulation.

“Uniform solutions are not achievable or desirable,” declared an attendee. “Uniformity is a techie dream, not a social one. Technology is more adaptable then mentality.” The sentences sound like Soviet propaganda slogans. This made it all the sweeter when the person finished his remarks citing Vladimir Lenin: “Trust is good; control is better.” Just as this conference report began by citing Reagan quoting a Russian proverb, thus it ends. “We believe here, too, Lenin was wrong,” the participant concluded.

Conclusion: Jaywalking on a Chaotic Sea

Trust is something one usually takes for granted when one has it, and really only appreciates the importance of when it is betrayed. Trust is measured in degrees, not absolutes. It is a process, not a state. It ebbs, decays and (hopefully) is restored. There is no one optimal way to establish or maintain it.

But what is most important is that it generally comes from interpersonal relationships – which makes all our attempts to foster it in virtual settings really an exercise in trying to simulate the dynamic of person-to-person rapport via technology. This, whether we are interacting with humanesque avatars in a virtual world, or watching the eyes on the screen of Air Force commander mannequins (as one example of trust-systems during the Cold War had it), to mimicking our real-world social network virtually, to deferring to brands, which are nothing more than public faces of companies we trust.

Is this sort of trust feasible in a global setting, when cultures are so different? Or, in the formulation of one participant, “Will the Swiss Germans learn to jaywalk a little,” because of their proximity between the more frenetic French and Italians? Indeed, the notion of jaywalking highlights another dimension relevant to government authority and trust: societies are based not only on adherence to rules, but on their pervasive minor disregard as well. A little rule-breaking is probably a good thing. Overly rigid rules lead to social and technical stasis. That’s the fear with an overly governmental approach to Internet issues – that it may never be timely with the state of technology, and thus can undermine progress and innovation. As one participant suggested: One generation’s buccaneers is another’s national navy.

If the Swiss Germans do learn to jaywalk a little, what does that say about the rest of us? Will people accept some loss of privacy online? (We probably have already!) Will we come to tolerate a certain level of spam? (We probably have little choice!) Will the Internet become an interconnected network of open networks and gated communities? Considering that the largest ISP today can be said to be Vodafone, the wireless phone operator, this heterogeneity is likely a persistent feature of the future. How we have an open, democratic debate about the merits of this, is unknown. The Internet, in some attendee's views, is going down the route of the Japanese trading company model, where there are sub-networks of trust; those on the outside must fend for themselves.

How rules will be established in such a world unearthed divergent perspectives. Rueschlikon participants were polled on their views of the future (see table, below). There was a slight difference between predictions and preferences: the majority hoped that there would be a "chaotic sea" of rules set among nations, international institutions, and private-sector initiatives, yet slightly more predicted that national regulations would hold greater sway. Strikingly, only one person believed some form of supranational body would end up setting rules, and ought to.

Survey: Number of attendees that predict or favor that by 2015, global Internet regulations will be established by:

	Predict	**Favor**
Nat'l regs:	**15**	**8**
Internat'l orgs:	**1**	**1**
Chaotic sea:	**13**	**20**

Nat'l regs: Mainly national regulations (i.e. state sovereignty still reigns).
Internat'l orgs: International organizations (i.e. harmonized intergovernmental accords).
Chaotic sea: Amalgam of national, international and private-sector-based policies.

If the predictions come to pass, and we end up with a jumble of rules, how would that form of Internet regulation be different than today? The answer depends on whether one believes such overlapping regulations and responsibilities could be effective. If so, it would resolve two classic problems bedeviling Internet policy, that of legitimacy and coherence. The first, legitimacy, entails who sets rules, what the rules are, and how they are imposed. The second, coherence, concerns how any one policy group relates to the others. Settle these two challenges, and a large part of Internet governance is resolved, too. However, if the heterogeneity of rules and roles isn't effective (that is, if it continues to be as cumbersome as today), then we can expect to remain in a twilight of uncertainty, with the potential of e-commerce stagnating until trust mechanism are eventually cobbled together piecemeal. Industry and users will surely muddle through, only more slowly than would otherwise be the case.

Taken together, the Rueschlikon 2004 discussion on openness, trust and sovereignty ultimately concerned the question of whether the Internet will remain global, or if the network may evolve in a way that it is locally optimized. The latter is more likely; even international companies that strive for global efficiency are locally based and must conform to local law. There is little evidence the Internet will be any different. What we can hope for is to find the right balance.

Moreover, the Internet was designed to be decentralized and anarchic because it was the right design for its purpose at the time, to survive a nuclear strike. But it is not the approach many might take if it were to be built today. The network also embodies a set of values constructed into the architecture, which expresses its US origins. Those attributes – low barrier to entry, low cost, free-flow of information and widespread connectivity – are under threat as the Internet spreads globally to societies that may not share these principles.

It raises the question how long the world will continue with the current mix of attempts to impose national controls in tandem with stealth activities to subvert those controls. The day may come when a failure to reach a balance will lead to an international confrontation and the need for a formal intergovernmental debate. The only way that can take place is if there were an identified international venue for those discussions to occur – and then, would a single institution or process be appropriate, or a balance of private self-regulation and governmental action? The question seems intractable for the moment. The poll's small vote in favor of intergovernmental accord shows little interested in going down that path. Still, proposals such as using Internet addresses to indicate what legal venue is appropriate can address some issues, and defer the day a global solution will gain momentum, for a single, unifying Internet law.

In the short term, it is likely we'll see a landscape of trusted intermediaries that take two forms. First, a trust interpreter, a company that determines the trust values in other countries, like language interpreters do for communication. Second, an intermediary for international agreements – a company that has relationships with consumers in different jurisdictions and offers that to e-commerce firms. They will be cultural shock-absorbers that act across boarders, similar to the role played by credit card companies for payments anywhere in the world. The question becomes how to regulate these trusted intermediaries. In five years' time, there may be a lot of trusted intermediaries, but likely the same questions.

It is true that people under 25 years old today may have different perspectives on these issues than the silver-haired folks wringing their hands and placing their policy bets. But it's also true that today's 17-year-olds eventually become 40-year-olds, and their perspectives change as they mature. The Rueschlikon participants themselves have evolved: As one long-time participant noted, after four years of dialogue together, attendees have developed a great deal of trust and openness among each other.

It is a testament to the work of the conference's co-organizers, Lewis Branscomb and Viktor Mayer-Schönberger, and to the generosity and interest of Swiss Re in providing a platform for opinion leaders at their Centre for Global Dialogue. Jaywalking on a chaotic sea, where trust is not assured, can be dangerous. Yet to deviate from Rueschlikon rules forbidding attribution and to quote Lewis: "The data points to pessimism but I chose optimism because optimism is more fun."

About the Author

Kenneth Neil Cukier, the author of this essay, covers technology and public policy for *The Economist*. From 2002 to 2004 he was a research fellow at the National Center for Digital Government at Harvard University's John F. Kennedy School of Government. This essay represents a critical synthesis of the discussions at Rueschlikon 2004; where views are expressed, they are his own.

The 2004 Rueschlikon Conference Participants

Steve Abernethy *President & CEO, SquareTrade*

Thomas W. Aust *VP and Senior Analyst, JP Morgan Investment Management*

Bernard Benhamou *Head, Forecast & Internet Governance, Prime Minister's Office, France*

Lewis M. Branscomb *Professor emeritus, Kennedy School of Government, Harvard University*

Gilles Bregant *Secretary General of the Mission for Digital Economy, Ministry of Economy, Finance and Industry, France*

Hans Peter Brondmo *Entrepreneur & Fellow, Digital Impact*

John Browning *Director / Contributing Editor, Basic Cat / Wired, United Kingdom*

Herbert Burkert *President, Research Center for Information Law, University of St.Gallen*

David Clark *Senior Research Scientist, MIT Laboratory for Computer Science*

Philip Evans *Senior VP, Boston Consulting Group*

Edward Felten *Professor, Princeton University*

Tamar Frankel *Professor of Law, Boston University School of Law*

Adam Golodner *Director, Global Security and Technology Policy, Cisco*

Fritz Gutbrodt *Head, Swiss Re Centre for Global Dialogue*

J.C. Herz *Researcher & Designer, University of Southern California's Center for Public Diplomacy*

Reid Hoffman *CEO, LinkedIn*

Raph Koster *Chief Creative Office, Sony Online Entertainment*

Olof Lundberg *former Chairman & CEO, Globalstar LP*

Lucy P. Marcus *Founder & CEO, Marcus Venture Consulting & HighTech Women*

Chris Marsden *Internet Governance Researcher, Oxford Internet Institute*

Viktor Mayer-Schönberger *Associate Professor, Kennedy School of Government, Harvard University*

Richard H. Murray *Chief Claims Strategist, Swiss Re*

Mike R. Nelson *Director Internet Technology & Strategy, IBM*

Eli Noam *Professor and Director, Columbia Institute for Tele-Information (CITI), Columbia University*

Morgan O'Brien *Vice Chairman and co-founder, Nextel Communications*

Anthony G. Oettinger *Founder & Professor of Applied Mathematics and Information Resources Policy, Program on Information Resources Policy, Harvard University*

Avner Offer *Chichele Professor of Economic History, Oxford University*

Cory Ondrejka *VP of Product Development, Linden Lab*

Otto Petrovic *Professor / Chairman, University of Graz / Evolaris Foundation*

William J. Raduchel *Former Chief Technology Officer, AOL/Time-Warner*

Reto Schnarwiler *Deputy Head Strategy Development, Swiss Re*

Peter Seipel *Dean & Professor, Stockholm University School of Law*

Sachio Semmoto *Founder, Chairman & CEO, eAccess*

Michael Siegrist *Professor for Human-Environment Interaction, ETH Zürich*

H. Brian Thompson *Chairman, Comsat International*

Herbert Ungerer *Advisor, Directorate General Competition, European Commission*

Hal Varian *Professor School of Information Management & Systems, UC Berkeley*

Peter Jon von Lehe *Deputy Head, Private Equity Fund of Funds, Swiss Re*

Kevin Werbach *Founder, Supernova Group LLC*

Yury Zaytsev *Group Information Officer & Member of the Executive Board, Swiss Re*

Note: Affiliations are listed for identification purposes only.