Chapter 1

Core Documents

Rob Atkinson, director of the Progressive Policy Institute's Technology, Innovation, and New Economy Project, suggested in the spring of 1999 that we co-author a briefing paper based on my interest in using digital certificates to both facilitate online democracy and stimulate the e-economy. The result was this essay, which is also available online at:

http://www.ppionline.org/ppi_ci.cfm?contentid=1369&knlgAreaID=107&subsecid=126.

Jump-Starting the Digital Economy (with Department of Motor Vehicles-Issued Digital Certificates)

June 1999
Marc Strassman and Robert D. Atkinson

The emerging digital economy promises high-productivity, low-unemployment, and increased standards of living. However, citizens, companies, or governments will be unable to fully realize these benefits until individuals can easily and securely authenticate themselves over the Internet.

Currently, few Americans can do this; that is, they are unable to fully represent themselves over the Internet in a way that securely tells other people and companies that they are who they claim to be and allows them to be taken seriously when they state their intentions. As a result, few companies or governments have developed applications that could use online authentication; and likewise, since few online applications require authentication, consumers have little reason to obtain the means to sign documents digitally. The Progressive Policy Institute (PPI) proposes that state governments should help jump start this process by providing digital certificates to all citizens who want them through state Department of Motor Vehicles (DMV) offices.

Just as we couldn't do business of any kind--educational, commercial, or interpersonal--if everyone walked around under a mask, it will be impossible to take full advantage of the Internet's power to collect, store, and distribute information, and therefore conduct various types of transactions, until each of us can authenticate ourselves online.

Authentication is an issue not unique to the Information Age. Medieval princes could secure and authenticate their documents with hot wax and a signet ring, ensuring that the message could not be tampered with without the recipient knowing it. Today, corporations and governments use official stamps and seals to signify the authenticity of the documents they issue. Similarly, digital signatures can be used to identify and authenticate documents and other files transmitted over the Internet.

The analogy between hot wax and signet rings and digital signatures is really very close. The engraved images on the signet rings were the product of some of that time's most advanced technology, engraving and metal work. Only the rich and powerful had access to the tools to insure the security and privacy of their data transmissions.

While digital signatures are based on an idea similar to the medieval signet rings, unlike the rings, digital signatures are potentially available to everyone. Using some of the latest computer and encryption technologies, digital signatures reduce a message to gibberish when it is tampered with, making it clear that the integrity of the document has been compromised, and allowing the recipient to disregard it.

Digital signature technology can be used to transfer into cyberspace the same, or a higher, level of assurance for legal and commercial purposes than has existed in common law, statutory law, and Uniform Commercial Codes for non-cyberspace transactions. By unambiguously and definitively establishing that a certain document has been "signed" by someone--or that someone has stated, indicated, and memorialized his or her intent to enter into an agreement of some type--digital signature technology makes it possible for binding transactions that cannot be repudiated to take place at a distance electronically. In short, digital signature technology enables today's e- commerce (online retailing) to flower into e-business and e-government (online transactions of a wide range).

What Are Digital Certificates and Digital Signatures?

To understand the applications and implications of digital certificates and digital signatures, it is important to understand what they do and how they do it.

First, think of the digital certificate as a pen used to write a digital signature. It is a unique digital code--a sequence of letters and numbers--that exists on a person's computer or smart card, that enables online identification. Certificates are provided by private companies that serve as certificate authorities (CA).

Then, think of a digital signature as the online equivalent to a signature you write with the pen. It is an encrypted and uniquely identified transmission that is attached to a signed document that becomes unintelligible if tampered with.

Here's how it works:

A person's digital certificate resides on their computer hard drive (or smart card). When a user wants to send a secure message or make any kind of online transaction requiring a digital signature, all he or she needs to do is access their certificate by clinking the appropriate icon on their Internet browser and entering their unique password. Employing the user's certificate, the computer will digitally "sign" a digest (an attachment to the document that the computer encrypts, or scrambles,

using the sender's digital certificate). The signature is then added to the core document along with a "public key" that enables a certificate authority (CA), a trusted institution charged with supervising this process, to authenticate the signature.

When the message is received, the recipient checks with the CA to determine if the public key he or she has received is in fact the proper public key of the person sending the message. The recipient can then be assured that the message has indeed been "signed" with the claimed sender's digital signature. All of this, fortunately, is done by the computers in the background and is invisible to the user.

Using unique digital certificates to create digital signatures also allows both the sender and recipient to know for certain that the received message is identical to the sent message and that it hasn't been tampered with between its transmission and receipt.

It is important to note that the use of encryption for authentication does not raise the same law enforcement policy concerns presented by the use of encryption for confidentiality since only the digest, and not the message, is encrypted, and because the digest can be read by anyone using the sender's public key.

Online Authentication is Critical in Driving the Next Wave of E-Business and E-Government

Today, virtually all of the approximately $80 billion in annual consumer-based e-commerce involves transactions that do not require the user to authenticate him or herself. For example, buying a book from Amazon.com does not require that a person prove to Amazon that they are who they say they are; it simply requires that they provide a valid credit card number.

However, for a truly digital economy to fully emerge and provide the kinds of productivity and standard of living increases that are possible, a host of functions now conducted in-person or on paper must be able to migrate to cyberspace where transaction and processing costs will be a fraction of their current levels. For example, applying for a bank loan by phone costs $5.90, but using the Internet costs 14 cents. Similarly, the cost of a teller transaction at a bank is $1.07, while online it is one cent, and filing taxes online is at least 60 percent cheaper than filing paper copies.

A whole host of functions will depend on digital signatures if they are to be conducted online efficiently and on a widespread basis. These include applying for a loan or insurance; filing legal documents; applying for a permit, driver's license, passport, or other official government document; paying taxes; and even voting electronically. In short, a large share of transactions that now require our signatures for some form of identification could migrate to cyberspace--but only if digital certificates are in widespread use.

Yet, important as digital certificates and digital signatures are to the full development of e-business and e-government, they are not yet widely in use or even widely discussed. Melissa the MacroVirus got more publicity in three days recently than digital certificates have received in the last three years. The main reason for this is that digital certificates and their relation to digital signatures is neither self-evident nor easy to understand. As a result, the media tend to shy away from the subject.

The complexity of these tools and the relative difficulty of obtaining them has meant that few people have them. Without widespread adoption by consumers, and with businesses apparently proceeding satisfactorily without them, few companies or governments have developed applications that could use online authentication. Likewise, since there are few online applications that require authentication, consumers have little reason to obtain these certificates. Moreover, putting digital certificates on smart cards (a credit card-shaped piece of plastic that contains a microprocessor for performing calculations, and a certain amount of computer memory for storing data) only becomes a viable proposition if there are sufficient smart card readers in use to attract enough users to support them. The chicken-and-egg metaphor is the simplest way to describe the problem. The overall result is the one we confront now: hardly any smart cards or digital certificates are in use anywhere in the United States.

Nevertheless, increasingly powerful applications will become possible as we move deeper into the Information Age, and many of them can only be put in place, or put in place effectively, by using smart cards, digital certificates, and digital signatures.

Accelerating the Adoption of Digital Signatures

As powerful and useful as digital signature technology is, there are certain obstacles standing between where it is now and where it could be. Principally, there is the problem of properly issuing the digital certificates upon which the entire system depends. Candidates for digital certificates, like applicants for driver's licenses, passports, or green cards, need at some point to present themselves before trusted authorities and establish their identity, either on the basis of a personal relationship with the trusted authority, or by presenting various types of documents that allow them to receive a digital certificate in their own name.

Some say that the provision of digital certificates should be completely left to the private sector. Clearly, the private sector needs to provide the technology, but it can also do this in partnership with government, the same way the private sector helps the government accomplish many of its tasks, from supporting a strong national defense to building roads.

Perhaps the most compelling reason why a government role is necessary for a robust implementation of digital certificates relates to the very significant economic benefits derived from breaking out of the chicken-or-egg conundrum faster than market forces alone are likely to be able to do. In particular, the lack of knowledge

of digital certificates--combined with the cost and inconvenience involved in asking millions of citizens to present themselves to separate "digital certification" agencies to establish their identity and apply for a digital certificate--means that the use of digital certificates will develop only slowly, at best.

Not only will this mean that a host of e-business applications will be slow to develop, the same will also be true for many e-government applications. Perhaps the strongest motivation for states to make it easy for citizens to obtain digital certificates is that these will go a long way in enabling the electronic delivery of government services. If citizens could use their digital certificates to interact with state and local governments, the efficiencies resulting from online and electronic transactions would allow government to more than recoup the costs associated with providing the certificates. For example, citizens could apply for licenses and permits, file taxes, submit regulatory and other legal forms, and even vote online. Not only would state and local governments save millions, but citizen satisfaction with government would increase.

Fortunately, there already exists in every state and almost every community an agency whose job it is to establish and verify the identify of persons, and to capture that identity with a picture. This agency collects and stores what those in the identification business call "biometric indicators," such as height, weight, eye color, and hair color. They test your vision. They ask for your address. They make sure they know when you were born.

The Department of Motor Vehicles is already collecting quite enough information about each person to issue him or her a digital certificate. In fact, one can argue that it is the DMV that plays the baseline function of establishing authentication in the physical world. DMVs issue millions of driver's licenses and non-driver identification cards every year that people use to establish their identity in a myriad of applications. There is no reason why they shouldn't play this role in the cyber world. In fact, VeriSign, a leading provider of digital certificates, states: "Think of Digital IDs as the electronic equivalent of driver's licenses or passports that reside in your Internet browser and e-mail software." And indeed, the level of technological sophistication of the cards that embody these licenses varies from state to state. In many states, such as California, these cards include a magnetic strip, a digitized photo, and a surface hologram, designed to thwart illegal modification of the card or the data it holds.

Given that state DMVs already have sufficient data to issue digital certificates, that they already issue cards used for identification, and that they already employ sophisticated electronic and anti-tampering technologies, these agencies are well positioned to issue digital certificates as part of their ongoing citizen identification and certification functions. And since they already carry out their work on a rolling basis, with staggered renewals of their cards designed to balance the work flow, expanding their role to one of establishing identity in the cyber world would mean a gradual and smooth introduction of this technology.

To maximize the usability of such Government-Issued Digital Certificates (GIDCs), every citizen/customer/user who elects to could receive their driver's license on a smart card, which in addition to a photo and printed information on its surface, would also contain a microprocessor and have the capacity to accept and store a digital certificate. Citizens/users would select their own passwords and--from their own computer at home or at work, or from a publicly provided one in a school, library or kiosk--generate and download their own unique digital certificate and private key.

This digital certificate would be a general-purpose digital certificate. There would also be room in the smart card for the user to allow other institutions, organizations, and companies to add "cardlets" that would entitle the cardholder to access his or her HMO records, to download e-cash, or to vote in elections. In order to assure security, these cardlets would be acquired by the holder on the basis of their general purpose digital certificate and whatever additional information other organizations or individuals required for access to specific databases or transaction opportunities.

People without computers could still use the digital certificates in their smart cards in various offline ways, such as for applying for government permits at a public computer kiosk. Credit card companies would perhaps become one of the organizations providing specialized cardlets for the smart cards. The potential of smart cards loaded with digital certificates to improve access, cut costs, and improve the efficiency of transactions that individuals conduct in the physical world is significant.1

In addition to providing the digital certificate to everyone on his or her driver's license or smart card, the state could also make the certificate containing the private key available directly to users to store on their computer(s) at home or at work, or both.

Likewise, this baseline authentication could be used to acquire other certificates that could be used for other purposes. Just as the driver's license is not the only means of personal identification, particularly for transactions with greater potential liability, other digital certificates issued by the private sector would also be used. With both smart cards and browser-based digital certificates, users would have private passwords that would prevent others from using their certificates to impersonate them in cyberspace.

As for the risk and liability questions surrounding the issuance and use of digital certificates in smart cards, there is a "defense in depth" approach that can effectively address this issue.

To start with, smart card and digital certificate users ("subscribers," in the industry jargon) are allowed to make up their own passwords. This reduces their need to

write them down on their card. If they do make this mistake, and if their card is stolen and used fraudulently, the subscriber is liable, since the card issuer exercised due diligence in seeing that it would not be misused. However, since the leading digital certificate system employs a Certificate Revocation List (CRL) technology, once one of their subscribers reports his or her card lost or missing, it can be revoked immediately, and anyone trying to use it will not be able to do so. This is like revoking a credit card, only faster and more certain.

The ability to instantly revoke a certificate also comes into play in the case of cards that are stolen and then attacked to discover their password. In addition to the revocation protection, the cards themselves are resistant to forced intrusion. Ten thousand computers working simultaneously for 22 hours are required to break a 56-bit key. Current cards employ 128-bit keys, and future versions will feature 256-bit keys, so it will take much longer to intrude into these--far longer than the time it takes to revoke the card entirely.

As for the previously mentioned private-sector participation, it makes sense for each DMV to outsource the actual provision of the digital certificates and the smart cards, as well as the management of the certificates, to one or more private companies with established track records in developing, deploying, and managing digital signature technology. In the same way that state governments hire private companies to supply copying or phone services, or even today's driver's licenses, they would contract with established digital signature technology companies to provide the necessary components required to introduce and maintain the processes that constitute the digital signature system. Moreover, they could choose whatever parameters and technologies for authentication they think work best and are most cost-effective. In fact, different states may use different technologies.

Finally, the fact that DMVs would issue these cards would in no way prevent individuals who would rather obtain certificates from private providers from doing so. Rather, it would simply make it easier for individuals to obtain them. In addition, just as individuals now use multiple forms of identification (such as passports, birth certificates, and witnesses) for certain transactions--especially more sensitive ones (e.g., papers that need to be notarized)--some individuals would likely obtain multiple digital certificates that could be used in combination or individually, but the DMV-issued certificate serving as a baseline.

A Threat to Privacy?

Aren't digital certificates a step toward a national ID or a potential threat to privacy? Personal privacy has long been a core American value, and the proliferation of modern database technology has done nothing to eliminate this concern. In fact, it has only made it a more pressing matter.2 Banks, merchants, HMOs, and the government all possess a lot of data about us and our habits, a fact that will not change in the presence or absence of a satisfactory means of issuing digital certificates.

Moreover, obtaining digital certificates from the DMV would be voluntary, and the state government would not itself serve as the certificate authority or know the passwords individuals choose to access the certificates. Also, just as driver's licenses are issued by states and not the federal government, under this proposal states would also issue digital certificates.

Finally, just as there are some transactions in the physical world that are anonymous and some that require identification, the same is true in the cyber world. Through the process of "anonymous authentication"--developed to allow voters to be authenticated online while maintaining the confidentiality of their electronic ballots and preventing their choices from being personally associated with them--other subscribers can also authenticate themselves as necessary while preserving certain aspects of anonymity in various other types of transactions. It will be important for state and local government to not require personal identification online when simple authentication will do. For example, a county may require that someone prove they are a resident before accessing a data base. In this case, a digital certificate would certify only that the person is a resident without revealing his or her identify. Fortunately, the technology is flexible enough to easily accomplish this. In addition, DMVs and the private digital certificate providers should establish a code of privacy that keeps the data they collect private. Overall, clearly thought out and reasoned government policies should prove sufficient in most cases to address these and other similar concerns.

Summary

It would not be an abrupt change for state DMVs to begin issuing driver's licenses on smart cards, and to provide the means for each citizen who wants to to create and store a digital certificate on that card. It would be, instead, an incremental modernization which will set the stage for a rapid advance in efficiency and cost-saving within state government, for an explosion of e-commerce, and for the facilitation of countless everyday tasks for every certificate holder.

Endnotes

1. For example, one potential application for smart cards would be to enable consumers to register online for hotel reservations, and download the room key code to their smart card, which could then be used to enter the room without registering at the front desk.

2. See Randolph H. Court and Robert D. Atkinson, Online Privacy Standards: the Case for a Limited Federal Role in a Self-Regulatory Regime, Progressive Policy Institute (March 1999).

Marc Strassman is the Executive Director of Campaign for Digital Democracy, a leading advocacy organization supporting the right of every citizen to vote and sign initiative

petitions over the Internet. He is also President of VoteSite.com, a private company providing Internet voting services to government jurisdictions and Internet initiative signing services and products to initiative circulators. Robert Atkinson is director of PPI's Technology, Innovation, and New Economy Project.

More than a year later, at a conference on “Internet Voting and Democracy,” at Loyola Law School in Los Angeles, California, I had a chance to raise the issue of digital certificates for electoral and other purposes with California Secretary of State Bill Jones.

Bizarrely enough, in light of my strong advocacy, in the article above, in June, 1999, of having the DMV issue digital certificates for use in Internet voting and also e-commerce situations, Secretary of State Jones took it upon himself to condescendingly lecture me on the fact that digital certificates would need to be issued by the DMV and that they could be used for a lot more than Smart Initiatives.

You can see and hear him responding at:

http://sfm.lpbn.org:8080/ramgen/bjq.rm?usehostname

This is the text of the California Internet Voting Initiative, drafted during 1999, and never circulated. It did not contain a provision for signing initiative and other official petitions over the Internet. It does contain a detailed list of requirements for any certified Internet voting system, in Chapter 2, Section 16956, Subsections (a) through (s). Any subsequent Internet voting system will probably need to meet all these requirements and maybe additional ones.

California Internet Voting Initiative

INITIATIVE MEASURE TO BE SUBMITTED DIRECTLY TO THE VOTERS

The Attorney General of California has prepared the following title and summary of the chief purpose and points of the proposed measure:

INTERNET VOTING, VOTER REGISTRATION, AND PETITION SIGNING. INITIATIVE STATUTE. Legalizes use of the Internet for purposes of voter registration, petition signing, and voting. Specifies criteria for any lawful Internet voting system. Requires Secretary of State to accredit means of identifying and authenticating voters. Requires counties to offer all voters Internet voting option. Specifies periods for Internet voting. Establishes right to register to vote over the Internet. Re-iterates responsibility of election officials to continue offering non-Internet options for voter registration, petition signing, and voting. Criminalizes any effort to interfere with the lawful operations of any Internet-based election system and specifies punishments.

TO THE HONORABLE SECRETARY OF STATE OF CALIFORNIA

We, the undersigned, registered, qualified voters of California, residents of _____ Country (or City and County), hereby propose amendments to the Constitution of California (the _____ Code, related to _____) and petition the Secretary of State to submit the same to the voters of California for their adoption or rejection at the next succeeding general election or at any special statewide election held prior to that general election or otherwise provided by law. The proposed statutory amendments (full title and text of the measure) read as follows:

PROPOSED LAW
The California Internet Voting Initiative

SECTION 1. It is the intent of the People of California in enacting this act to legalize the use of the Internet for voter registration, the signing of petitions, and the casting of ballots in all elections conducted by public entities in California, in order to promote broader participation in the state's electoral processes. To implement this goal, it is the intent of the People of California to do the following:

(a) Authorize the use of the Internet for election purposes, including voter registration, petition circulation, and the casting of ballots.

(b) Require the Secretary of State, within 90 days of the enactment of this act, to develop and adopt standards according to which the Internet may be used for these purposes.

(c) Allow for the casting of ballots, the registration of voters, and the collection of signatures on petitions by electronic means over the Internet during the timeframe established by law.

(d) Minimize the wrongful manipulation, fraudulent use, or violations of the integrity of the means by which the Internet is used for these purposes by requiring Internet voting systems to employ suitable technologies and practices, and establish suitable sanctions against those illegal acts.

(e) Adopt a policy of providing all voters with suitable means of identifying and authenticating themselves over the Internet in order to perform the electoral functions covered by this measure.

(f) Adopt a policy of providing suitable means of assuring the confidentiality of information

communicated under this bill.

SEC. 2. Division 16.5 (commencing with Section 116950) is added to the Elections Code, to read:

DIVISION 16.5. USE OF INTERNET FOR ELECTORAL PURPOSES

CHAPTER 1. GENERAL PROVISIONS

16950. (a) Notwithstanding any other provision of law, a qualified voter in this state may register to vote, sign a petition, and vote in a direct primary, statewide general, or special election using the Internet, using means that have been approved pursuant to Chapter 2 (commencing with Section 16955).

(b) The Secretary of State shall, within 90 days of the effective date of this division, establish all standards and adopt all rules and regulations required to be adopted by the Secretary of State under this division.

16951. For the purposes of this division:

(a) "election services" means the services related to elections, including voter registration, petition circulation, and the casting of ballots

(b) "petition" means in lieu, initiative, referendum, recall, and write-in petitions and petitions to the Office of Legislative Counsel for the drafting of initiatives

(c) "ballot" means an electronic record containing all of, and only, the candidates for local, state, or federal office, and the state and local measures for which the voter is entitled to vote, in whatever order is mandated by law

(d) "physical polling place" means a traditional, walk-in polling place

(e) "signatures physically collected on petitions" means manually-generated signatures collected on paper petitions and memorialized thereon in ink

(f) "electronically-signed petition" means an electronic record consisting of the text of a proposed initiative, together with other required text, and which has been signed by a registered voter using one of the means of identification and authentication approved by the Secretary of State under Section 16960 below

(g) "electronically submit" means to transfer securely over the Internet or to physically transfer by means of a device suitable for the storage and retrieval of electronically-recorded information

(h) "system for delivering election services over the Internet" means an assemblage of computer hardware, computer software, and network resources, together with the internal processes and operational procedures whereby these components are utilized in order to deliver election services

(i) "casting of ballots" means voting

(j) "system availability" means the percentage of the time during which a system responds appropriately to legitimate and authorized requests

(k) "master ballot information" means instructions for properly constituting the contents of ballots for the voters in a particular jurisdiction or set of jurisdictions

(l) "the Internet" means the global, inter-connected network of networks originating from the ARPAnet

16952. Unless a provision of this division expressly requires otherwise or is inconsistent with another provision of this code, each provision of this code that would otherwise regulate the casting of ballots, counting and reporting of ballots, circulation of petitions, or registration of voters shall apply to this division, including, but not limited to, any civil or criminal penalties associated with those activities, any duties imposed on state or local elections officials, and any established timeframes.

CHAPTER 2. ESTABLISHMENT OF STANDARDS FOR VOTING OVER THE INTERNET

16955. The Secretary of State shall establish standards for the use of the Internet for electoral purposes and shall approve and certify for use for these purposes systems that meet the

criteria set out in Section 16956.

16956. To qualify for use in an election, a system intended for such use shall demonstrate the existing capacity to do all of the following:

(a) Provide for the secure identification and authentication of each eligible voter utilizing the system.

(b) Provide for the secure identification and authentication of all elections officials, electoral jurisdictions and of all network servers, application servers and all other relevant components of the computing base used for elections by the elections officials and electoral jurisdictions supervising and responsible for voter registration, petition signing, or voting, as appropriate.

(c) Protect the confidentiality and integrity of each voter's ballot.

(d) Provide for the effective disassociation of the content of a voter's cast ballot from the identity of the voter casting it.

(e) Prevent the casting of multiple ballots in any election, the multiple signing of any petition, or multiple registrations as a voter by any person.

(f) Provide protection against tampering, fraudulent use, illegal manipulation, or other abuse by voters, elections officials, any other government agent or official, or any other individual, group, organization, or association of persons.

(g) Be as easy as possible to use by all voters and all election officials.

(h) Provide each voter with a ballot containing all of, and only, the candidates for local, state, or federal office, and the state and local measures for which the voter is entitled to vote, in whatever order is mandated by law.

(i) Provide the means by which voters may cast write-in votes in electronic form for candidates whose names do not appear on the ballot but who have qualified for write-in status.

(j) Provide at least 99.8 percent system availability during the electronic voting period established by law and for as long after the close of the voting period as is required in order to assure the full and complete communication of all ballot information.

(k) Be sufficiently scalable to provide voting access to all voters in the jurisdiction where it is employed, during the same hours when physical polling places are open for voting on election day.

(l) Be accessible to all voters, including all voters with disabilities, consistent with the Americans with Disabilities Act of 1990 (42 U.S.C. Sec. 12101 et seq.).

(m) Be capable of being upgraded as technology improves.

(n) Provide support for non-repudiation of all electronic electoral transactions (including voter registration, the signing of petitions, and the casting of ballots) between and among voters, elections officials, and electoral jurisdictions.

(o) Be readily available for an audit of its contents, results, and process by a competent accounting firm at a level sufficient to assure the integrity of the system and the public's confidence in its integrity.

(p) Be capable of securely transmitting information over a network.

(q) Be capable of hosting and operating an Internet website that can securely and accurately carry out all the elections functions authorized in this division to be conducted over the Internet and of securely and accurately transmitting all elections data (including that from registration forms, petitions, and ballots) collected and processed by it in performing these functions to the appropriate election authorities.

(r) Be capable of conducting recounts of ballots and electronically-signed petitions.

(s) Be capable of issuing electronic receipts to users to memorialize their registration, petition signing, or voting.

16957. (a) Before any system for delivering election services over the Internet may be used by voters, the Secretary of State shall perform the tests necessary to establish that the system in question conforms to the requirements of Section 16956 and the standards adopted by the Secretary of State pursuant to this division. The Secretary of State may contract with a recognized independent testing facility to perform the tests required by this section..

(b) The Secretary of State, or a recognized testing facility designated by the Secretary of State to perform the tests required by this section, shall examine each system proposed for use in the delivery over the Internet of election services and either accredit that it is fit for use or deny it accreditation within 90 days of its submission to the Office of the Secretary of State or to a testing

facility designated by the Secretary of State to perform the tests required by this section.

(c) If approval is denied, the denial shall specify in writing the reasons for the denial and what specific remediations or modifications must be made to the disapproved system in order for it to qualify for subsequent accreditation.

(d) The Secretary of State, or a recognized testing facility designated by the Secretary of State to perform the tests required by this section, may, at their discretion, require a fee to be paid by the owner of the system sufficient to cover the reasonable costs of testing it for compliance with the requirements of this section.

(e) Once the Secretary of State has accredited a system for use in the delivery of election services over the Internet, it shall be designated as accredited by the Secretary of State for use by voters and all electoral jurisdictions within the state and may, immediately upon this accreditation, be used for this purpose.

CHAPTER 3. ESTABLISHMENT OF MEANS TO IDENTIFY AND AUTHENTICATE VOTERS

16960. The Secretary of State shall identify and accredit means by which voters are able to identify and authenticate themselves over the Internet in order to securely access and use the election functions covered by this measure (voter registration, petition signing, and voting). These means may include, but are not limited to, the use of digital certificates and signatures, other electronic signature methods, or biometric means, including voice, iris, or retinal scans, fingerprints, or DNA prints.

CHAPTER 4. COUNTIES REQUIRED TO PROVIDE INTERNET ELECTION SERVICES

16969. Election officials in each county shall make available to all eligible citizens within their jurisdiction the means to register to vote, sign petitions, and vote over the Internet. Each county's election officials may, at their discretion, provide these Internet-based election services using their own staff and equipment or they may contract for one or more of them with one or more owners of an accredited system for delivering election services over the Internet. When a county chooses to provide one or more of these electoral services itself, the system it creates and uses to deliver these services must meet the same standards set out in Chapter 2 of this Section and be approved for that purpose by the Secretary of State or a recognized testing facility designated by the Secretary of State to perform the tests required in Chapter 2 of this Section.

CHAPTER 5. CASTING BALLOTS OVER THE INTERNET

16970. The Secretary of State shall develop and adopt rules and regulations governing the provision of master ballot information from each county to the system being used by that county to offer Internet election services and the transmission of registration information, electronically-signed petitions, and ballots cast over the Internet to local elections officials. The rules and regulations shall assure that:

(a) the system being used by a county to offer Internet election services shall provide a ballot to each voter choosing the Internet voting option that contains all of, and only, the candidates for local, state, or federal office, and the state and local measures for which the voter is entitled to vote.

(b) the ballots cast by, or at the instigation or direction of, any person attempting to cast more than one electronic ballot, or an electronic ballot and one or more other ballots at a physical polling place, by mail-in absentee ballot, or by any other means of voting, now or later to be authorized, with the intent to violate the integrity of the Internet voting system by casting one or more fraudulent ballots, or to unlawfully cast the electronic ballot of another voter, shall be disqualified.

(c) the identity and authenticity of the Internet voting system being used by voters is definitively established as part of the voting process.

16971. Any voter may vote using an accredited system for delivering election services over the Internet selected by their electoral jurisdiction, using one of the means of identification and authentication approved by the Secretary of State pursuant to Section 16960, during either:

(a) The same time period during which absentee ballots are accepted in that jurisdiction, or
(b) The same hours provided for voting at physical polling places on the day elections are held in that jurisdiction.

CHAPTER 6. ADDING BALLOTS CAST OVER THE INTERNET TO NON-INTERNET VOTES TO CALCULATE OVERALL TOTALS

16975. (a) At each election, the county shall tabulate the results of the ballots cast by voters within its jurisdiction over the Internet and add these results to its non-Internet voting totals to calculate the overall results.

CHAPTER 7. CIRCULATING INITIATIVE PETITIONS OVER THE INTERNET

16980. Any duly authorized petition may be circulated on the Internet, and any voter may electronically sign such a petition employing a system approved for such use under the provisions of this section, using one of the means of identification and authentication approved by the Secretary of State pursuant to Section 16960. Signatures so collected shall be as valid as signatures physically collected on petitions and the total of such signatures shall be added to the number of signatures collected for a petition by all other authorized means to calculate the overall results.

16981. Election officials may, at their discretion, provide a system for the collection of electronically-signed petitions using their own staff and equipment or they may contract with the owner of an accredited system for delivering election services over the Internet to do so. When a county chooses to provide the means of electronically signing petitions itself, the system it creates and uses to deliver that service must meet the same standards set out in Chapter 2 of this Section and be approved for that purpose by the Secretary of State or a recognized testing facility designated by the Secretary of State to perform the tests required in Chapter 2 of this Section.

16982. The circulators of petitions circulated on the Internet may collect electronically-signed petitions using an accredited system for delivering election services over the Internet and then may electronically submit the electronically-signed petitions to local election officials or, in the case of in lieu petitions pertaining to candidates for statewide office or of statewide initiative, referendum, or recall petitions, directly to the Secretary of State, as appropriate. The local elections official or the Secretary of State shall verify the electronic signature of each signer of a petition circulated on the Internet under the provisions of Section 16980, using the means of identification and authentication approved by the Secretary of State pursuant to Section 16960, consistent with other provisions of this code pertaining to the verification of signatures collected on initiative petitions.

16983. All electronic signatures of petitions generated by, or at the instigation or direction of, any person acting with the intent to violate the integrity of the Internet voting system by signing a petition more than once, or by signing in the name of another voter, or by otherwise fraudulently signing a petition being circulated on the Internet, shall be disqualified.

CHAPTER 8. INTERNET VOTER REGISTRATION

16985. The Secretary of State shall develop and adopt rules and regulations for the registration of voters over the Internet, using one or more of the means of identification and authentication approved by the Secretary of State pursuant to Section 16960. Counties may provide their own systems to perform the registration function, or they may contract with the owner of an accredited system for delivering election services over the Internet to do so. When a county chooses to provide the means for citizens to register to vote itself, the system it creates and uses to deliver that service must meet the same standards set out in Chapter 2 of this Section and be approved for that purpose by the Secretary of State or a recognized testing facility designated by the Secretary of State to perform the tests required in Chapter 2 of this Section.

CHAPTER 9. CONTINUATION OF NON-INTERNET BASED ELECTION SERVICES

16991. Nothing in this division may be construed to relieve local elections officials from providing registered voters, who so choose, with the opportunity to cast ballots or sign petitions, in the manner required by other provisions of this code or to continue to register voters, who so choose, in the manner required by other provisions of this code.

CHAPTER 10. PENALTIES

16995. Any person who interferes with the lawful operation of any electoral activity conducted electronically pursuant to this division with the intent of committing fraud or violating the integrity of any system used for these activities, including its internal code, contents, or results, is guilty of a crime for each occurrence, punishable by imprisonment in the state prison for 16 months or two or three years, or in a county jail for not more than one year, or a fine of not more than ten thousand dollars ($10,000), or by both that imprisonment and fine. In addition, as a condition of parole, any individual found guilty of a crime pursuant to this section may be prohibited from using any electronic network for a period of not more than the term of parole.

CHAPTER 11. DEFENSE OF THIS INITIATIVE

16996. The proponent(s) of this initiative shall have standing to defend this measure in court.

16997. Any challenge to this measure shall originate in the California Supreme Court.

SEC. 3. The Legislature shall amend and revise the Elections Code or any other related provision of law as necessary to further the implementation of Division 16.5 (commencing with Section 16950) of the Elections Code within the timeframes set forth in that division.

SEC. 4. The provisions of this measure are severable. If any provision of this measure or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provision or application.

This is the text of the Smart Initiatives Initiative, drafted during 2000, and now officially in circulation. To read it online, or to download a signable copy of it, go to:

http://www.smartinitiatives.org

To hear streaming video interview about the SII, go to the Smart Initiatives site, click through to the Media Wall, and click again on "Live, From New York, It's Smart Initiatives."

Smart Initiatives Initiative

INITIATIVE MEASURE TO BE SUBMITTED DIRECTLY TO THE VOTERS

The Attorney General of California has prepared the following title and summary of the chief purpose and points of the proposed measure:

DIGITAL SIGNATURE. ELECTION PETITIONS. PUBLIC AND PRIVATE TRANSACTIONS. INITIATIVE STATUTE. Establishes a state agency to issue a digital certificate to any California resident. Requires certificate to generate a verified digital signature that can be used to subscribe to any authorized public or private sector electronic transaction. Authorizes use as driver license, identification or voter registration card at no additional charge. Requires election officials to validate and count digital signatures for candidacy, initiative, referendum and recall petitions if transmitted to a secure website provided by candidate or proponent. Preserves traditional signature methods. Imposes imprisonment and fines for violations of this system. Summary of the estimate by Legislative Analyst and Director of Finance of fiscal impact on state and local governments: Measure would result in unknown, major one-time costs to develop the systems, and could result in unknown major (probably in the range of tens of millions of dollars) annual net costs to state and local governments.

TO THE HONORABLE SECRETARY OF STATE OF CALIFORNIA

We, the undersigned, registered, qualified voters of California, residents of _____County (or City and County), hereby propose amendments to the Elections Code and the Government Code, relating to secure online identification and petitioning, and petition the Secretary of State to submit the same to the voters of California for their adoption or rejection at the next succeeding general election or at any special statewide election held prior to that general election or otherwise provided by law. The proposed statutory amendments (full title and text of the measure) read as follows:

SECTION 1. This act shall be known and may be cited as the Smart Initiatives Initiative.

SECTION 2. Chapter 8 (commencing with Section 9700) is added to Division 9 of the Elections Code, to read:

CHAPTER 8. ELECTRONIC PROCEDURES

9700. (a) Notwithstanding any other provision of law, any petition circulated pursuant to this division may be signed using a digital certificate issued by the Digital ID Issuing Authority pursuant to Section 11790 of the Government Code.

(b) This section shall not be construed to preclude the collection of signatures for a petition by any other means authorized by law.

9701. (a) A proponent of a measure for which a petition is circulated under this division may collect digital signatures generated by digital certificate pursuant to Section 9700, by posting the petition at a website managed by the proponent for that purpose. A candidate for office may, under the provisions of this division, collect and submit signatures in lieu of paying all or part of a filing fee required to run for that office.

(b) A certificated copy of the petition, properly formatted and in compliance with all other standards required by this division, except as to signature spaces, shall be provided online to potential signers of it by displaying the document (other than its signature spaces) in a manner that securely presents an unalterable image equivalent to that normally required for paper versions of the petition, using document exchange and management software approved by the Department of Information Technology for this purpose.

[c] (1) The petition displayed as described in subdivision (b) shall provide a means whereby a user may generate a digital signature on the petition, using a digital certificate, as described in Section 9700, with software approved for this purpose. The signer shall also provide any additional information required by law.

(2) In order to prevent the submission of multiple signatures by the same individual, the computer system hosting the measure shall be programmed to accept only one digital signature generated by the single digital certificate issued to each eligible person, and to reject all subsequent efforts to sign the petition with that digital certificate.

(d) The identity of any person generating a digital signature on a petition pursuant to this section shall be protected as provided by law. No part of this chapter shall be construed to abrogate any right of privacy otherwise protected under law.

(e) Any person who digitally signs a petition pursuant to this section may withdraw that digital signature as provided in Section 9602, except that the request for withdrawal may be submitted by electronic means, using a digital signature generated by digital certificate.

9702. (a) The petition shall be submitted to the appropriate elections official for filing and validation either on electronic storage media delivered physically to the official or by transmission to the official over the Internet under secure conditions, as approved by the Department of Information Technology, at the discretion of the proponent.

(b) Notwithstanding any other provision of law, petitions for which digital signatures have been collected under this chapter may be filed with the appropriate elections official by the proponent, using the methods set out in Section 9702 (a), at any time prior to the final date for filing the petition and the digital signatures contained therein shall be validated or rejected by that elections official within three (3) working days of their receipt.

[c] Signatures generated by digital certificates under this chapter shall be validated by the elections official responsible for validating signatures for the petition in question, using the most rigorous methods of digital authentication available, in conjunction with, or using procedures approved by, the Digital ID Issuing Authority.

9703. (a) In the case of initiative, referendum, and recall petitions, any digital signature generated by a digital certificate and validated pursuant to Section 9702 shall be counted toward the total required to qualify the measure for the ballot in question. In the case of signatures to be collected and submitted in lieu of requiring a candidate for public office to pay all or part of a filing fee for that office, any digital signature generated by a digital certificate and validated pursuant to Section 9702 shall be counted toward the total required to exempt that candidate from having to pay all or part of the filing fee for that office. The tally of validated signatures collected shall be forwarded to the Secretary of State by the appropriate elections official on an ongoing basis.

(b) The Secretary of State shall provide and update information showing the number of validated digital signatures collected, based on the most recent information provided by the appropriate elections official or officials, at the official website of the Secretary of State.

9704. The Digital ID Issuing Authority and the Department of Information Technology may each adopt regulations to implement this chapter.

9705. (a) Any person who interferes with the lawful operation of the electronic processes specified in this chapter with the intent of committing fraud or violating the integrity of any system used for these activities, including, but not limited to, its internal code, contents, or results, by any means, whether or not through the use of a computer, or who attempts to impede access to an official petition website by means of a "denial-of-service" attack or by any other means, is guilty of a public offense for each occurrence, punishable by imprisonment in the state prison for a period of 16 months or two or three years, or in a county jail for not more than one year, or a fine of not more than ten thousand dollars ($10,000), or by both that imprisonment and fine.

(b) As a condition of parole, any individual found guilty of an offense pursuant to this section may be prohibited from using any electronic network for a period of not more than the term of parole.

SEC. 3. Section 16.5 of the Government Code is amended to read:

16.5. (a) In any written communication with a public entity, as defined in Section 811.2, in which a signature is required or used, any party to the communication may affix a signature by use of a digital signature that complies with the requirements of this section. The use of a digital signature shall have the same force and effect as the use of a manual signature if and only if it embodies all of the following attributes:

(1) It is unique to the person using it.
(2) It is capable of verification.
(3) It is under the sole control of the person using it.
(4) It is linked to data in such a manner that if the data are changed, the digital signature is invalidated.
(5) It conforms to regulations adopted by the Secretary of State. Initiation regulations shall be adopted no later than January 1, 1997. In developing these regulations, the secretary shall seek the advice of public and private entities, including, but not limited to, the Department of Information Technology, the California Environmental Protection Agency, and the Department of General Services. Before the secretary adopts the regulations, he or she shall hold at least one public hearing to receive comments.

(b) The use or acceptance of a digital signature shall be at the option of the parties, except as provided in Chapter 8 (commencing with Section 9700) of Division 9 of the Elections Code and as provided in Section 11791 of the Government Code. Nothing in this section shall require a public entity to use or permit the use of a digital signature.

[c] Digital signatures employed pursuant to Section 710066 of the Public Resources Code are exempted from this section.

(d) "Digital signature" means an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature.

SEC. 4. Chapter 7.5 (commencing with Section 11790) is added to Part 1 of Division 3 of Title 2 of the Government Code, to read:

CHAPTER 7.5. DIGITAL IDENTIFICATION ISSUING AUTHORITY

11790. (a) The Department of Motor Vehicles, the Secretary of State, the Department of Information Technology, and the county registrars of voters, shall

collaborate to establish the Digital ID Issuing Authority of the State of California, whose mission shall be to efficiently and cost-effectively provide California residents with a high-level digital certificate in an easy-to-use form.

(b) The Digital ID Issuing Authority of the State of California shall, either on its own or by contracting with a suitable private supplier or suppliers, develop, design, implement and maintain a system capable of establishing the identity of individuals with sufficient assurance to issue them the digital certificates called for in this division, of interacting with recipients of these certificates so as to allow them to personalize and secure for their sole use the digital certificates they are issued; of maintaining in good order the databases containing the digital certificates they issue and any other associated data necessary to the efficient functioning of the digital certificate system; of keeping this system current by adding new users as they are issued digital certificates, removing users whose certificates are revoked, or when a user becomes deceased or permanently relocates out of the state, and changing any relevant data about users in a timely manner; and of providing to all electoral and other state and local agencies, in an accurate and speedy manner, the authentication of the digital signatures generated by the certificates it has issued, whether in the context of official petitions, transactions with government, or transactions in the private sector.

(c) (1) The Digital ID Issuing Authority, in collaboration with each recipient, shall generate and issue an individualized digital certificate belonging solely to that recipient. Through the use of passwords, biometrics or other means, this digital certificate shall be rendered accessible solely to the person to whom it is issued, as specified in Section 16.5 (a) (3) of the Government Code, and cited in SEC. 3 of this division. The digital certificates created by the authority according to these procedures shall then be loaded onto smart cards that use the best generally available technology, and that shall be used as the substrate for the driver license or identification card issued by the Department of Motor Vehicles to each applicant/recipient of these licenses and cards, unless an applicant/recipient specifies that he or she does not wish to have either a digital certificate at all or does not wish to have a digital certificate installed on the smart card providing the substrate of their driver license or identification card.. A smart card containing the registrant's personalized digital certificate shall be provided to registered voters who have neither driver's licenses nor identification cards, as the substrate of their voter registration cards, unless the registrant specifies that he or she does not wish to have either a digital certificate at all or does not wish to have a digital certificate installed on the smart card providing the substrate of their voter registration card. Anyone eligible to receive a digital certificate on a smart card under the provisions of this division may, at their discretion, receive a smart card without a digital certificate as the substrate of the driver license, identification card, or voter registration card to which they are entitled. The smart cards provided under the provisions of this division may, as practicable, be "contactless," allowing their use at a distance, and may include optical storage areas, allowing users to store and retrieve large amounts of data on and from their cards. There shall be no additional fees charged to users (holders of driver licenses, identification cards, or voter registration cards) for the provision of the digital certificate or smart card.

(2) For purposes of this subdivision, the following definitions shall apply:

(A) "Smart card" means a card with a built-in microprocessor and memory that is capable of receiving, storing, processing, and transmitting electronic data.

(B) "Substrate" means the physical material of an identification card, upon which information is placed.

[c] As part of the process by which a holder personalizes his or her certificate and through which the Digital ID Issuing Authority establishes the identity of the holder, each holder of the state-issued digital certificate may request the Digital ID Issuing Authority to send the holder, free of charge, a complete and accurate digital copy of his or her digital certificate by electronic mail to up to and including ten electronic mail addresses provided by the holder. Pursuant to this subdivision, the digital certificate holder may request, as part of their allotted downloaded copies, that some of these copies be transmitted to cellular phones and/or other mobile or fixed wireless digital devices of their choice. The Digital ID Issuing Authority shall comply with all such requests.

11791. (a) A digital certificate issued by the Digital ID Issuing Authority pursuant to Section 11790 shall be accepted by any state entity that offers secure transactions over the Internet, as complete and adequate proof of an individual's identity, and as capable of generating a "digital signature," as defined in Section 16.5, for purposes of executing any form, document, or other instrument related to the transaction, and that digital signature shall be deemed to constitute that individual's assent to the terms of the transaction and shall be accepted as such by the state entity involved.

(b) A digital certificate issued by the Digital ID Issuing Authority pursuant to Section 11790 may be used for any personal or commercial purpose for which identification is required, and for generating a valid and acceptable legal signature as required, as provided under Title 2.5 (commencing with Section 1633.1) of Part 2 of Division 3 of the Civil Code.

11792. The Digital ID Issuing Authority and the Department of Information Technology may each adopt regulations to implement this chapter.

11793. (a) Any person who interferes with the lawful operation of the electronic processes specified in this chapter with the intent of committing fraud or violating the integrity of any system used for these activities, including, but not limited to, its internal, contents, or results, by any means, whether or not through the use of a computer, or who attempts to impede access to an official petition website by means of a "denial-of-service" attack or by any other means, is guilty of a public offense for each occurrence, punishable by imprisonment in the state prison for a period of 16 months or two or three years, or in a county jail for not more than one year, or a fine of not more than ten thousand dollars ($10,000), or by both that imprisonment and fine.

(b) As a condition of parole, any individual found guilty of an offense pursuant to this section may be prohibited from using any electronic network for a period of not more than the term of parole.

SEC. 5. (a) The California Supreme Court shall have original jurisdiction in any legal action or proceeding to challenge the validity of this act.

(b) The proponents of this act shall have standing to defend the act in any such action or proceeding.

SEC. 6. The Legislature may amend this act only by a statute passed by a two-thirds vote of the membership in each house of the Legislature that is consistent with and furthers the purposes of this act.

SEC. 7. The provisions of this act are severable. If any provision of this act or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provisions or applications.

Chapter 2

The IntellectualCapital.com Series

The IntellectualCapital.com Series

In the spring of 1999, Bob Kolasky, publisher of VoxCap, suggested that I write some material for their IntellectualCapital.com website. I ended up writing three pieces for them over four months: "Internet Voting Circa 2002," "Could the Internet Change Everything?" and "Putting the 'E-' in E-democracy".

You can also access these pieces online at:

1. Internet Voting Circa 2002
http://ic.voxcap.com/issues/issue228/item4339.asp
still available at: http://speakout.com/cgi-bin/udt/im.display.printable?client.id=speakout&story.id=3826

2. Could the Internet Change Everything?
http://ic.voxcap.com/issues/issue249/item5418.asp

3. Putting the "E-" in E-democracy
http://ic.voxcap.com/issues/issue294/item6421.asp

(links to all three papers can also be found at:
http://ic.voxcap.com/bios/bio956.html)

Internet Voting Circa 2002

Thursday, May 06, 1999

With the Internet becoming more powerful, prominent, cheaper and ubiquitous by the hour and with political participation levels lower than ever and sinking precipitously every election cycle, it only makes sense to consider fixing the latter by means of the former.

Protecting identities

Internet voting and its cousin, digital signatures on initiative petitions, are now seen by many observers as inevitable steps in a national effort to get people back to the polls or, more accurately, to get the polls out to the people.

How would Internet voting look in, say, the 2002 elections? Surprisingly, it would not look much different than ordering books at Amazon.com looks today, with the operative metaphor being a "digital ballot," instead of an "electronic shopping cart." The main difference would be that the security

and authentication levels would be higher, since we would be electing our officials and not just ordering mystery novels or other light entertainment.

The standard Internet voting system would require each voter to have a "digital certificate," an advanced type of account number that is capable of "digitally signing" any document generated by a computer, including an Internet ballot. During the digital signing process, the ballot would be encrypted so that it cannot be read (or altered) while in transit to the "virtual polling place" (the server used by the electoral jurisdiction).

When it arrives at the official server, this powerful computer would retrieve the voter's "public key" from a trusted Certificate Authority and use it to decrypt the encrypted ballot. If the ballot file decrypts coherently, the official server will know two things: it was sent by the person who signed it, and it has not been tampered with since he or she signed it.

Authenticated identity and non-tampering are the two most important things that need to be established by the Internet voting system. The use of digital certificates to generate digitally signed ballots makes it possible to determine both the identity of the sender and the integrity of the ballot to a degree of certainty far exceeding that which what now exists with the often almost-informal means used for brick-and-mortar voting.

The other important and necessary feature in an Internet voting system is a way to ensure the anonymity of the ballots' content so that no voter can be associated with the way he or she voted. The standard Internet voting system of 2002 will achieve this by first authenticating the voter's identity, removing his or her name from the list of voters eligible to vote in that election, stripping his or her identifying information off the file, then sending the file to the tabulation server for aggregation and counting.

On Election Day ... or Days

That is how the technology will work, but what about the experience of going to the ballot box?

By 2000, state Departments of Motor Vehicles will issue driver's licenses and state identification cards on "smart cards," credit-card-size objects with a computer chip and electronic memory inside them. Pre-loaded on these smart cards will be each person's unique digital certificate. These digcerts also will be sent by e-mail from the DMV to

the computer(s) of everyone who asks for them. The smart cards will now be in the hands of everyone eligible to vote, since they will be generated and provided, at no additional cost, to everyone who has any form of state identification.

During the election period (starting two weeks before Election Day and ending at 8 p.m. on that day), voters with access to the Internet will visit the election site (at, say, http://www.votesite.net), and enter their names and addresses. This will allow the system to determine their precincts and to generate and deliver personalized electronic ballots that correspond to their places of residence, and include all the candidates and ballot measures that voters in that district are entitled to vote on.

The actual voting process will take less time than it does now. By clicking in a box next to a candidate's name, or by clicking on the candidate's name itself, the voters will make their selections. Similar clicking will allow the voters to express a "Yes" or "No" preference on each ballot measure. Voters can skip around, return to any section, or change their votes. When they are finished making their choices, they click on the "Finished" button, which causes the system to display all their selections for their review and approval. They can still make changes to any of the items.

When the voters are satisfied with their choices, they click on the "Submit" button, and that's it. A "digital ballot" file containing their selections is then created and "digitally signed" by their digital certificate and sent to the electoral server.

There, using the voter's public key, it is de-crypted, the voter's name is removed from the list of voters eligible to vote in that election, all identifying information is stripped off, and it is sent to the tabulation server, where it will be counted.

What about those left behind?

There are two groups that might be left behind by the adoption of digital voting: communities (including nations) with little penetration of technology and individual voters without access to computers.

For entire states that lag behind in the transition to electronic voting, the consequences may be dire. Because the digital-voting infrastructure also enables e-commerce at a high level, jurisdictions that tarry while others move forward will suffer the inevitable effects of being unable to compete effectively, economically, culturally and in terms of quality of life.

What about voters without computers in jurisdictions with electronic

voting? They will go, as they always have, to their local polling place. There, they will enter a voting booth containing an "Internet Voting Appliance" (IVA) ©, a specialized laptop computer that contains a slot for a smart card, a touch screen for input and a wireless Internet connection for transmitting ballots. The process here will be essentially identical to that experienced by voters who use their own computers at work or at home -- access to a Web site is access to a Web site, however achieved.

Once the proper ballot appears on the IVA, the mobile voters will make their choices just as their at-home or at-office counterparts will do. When they are finished making their selections, they, too, will click on the "Submit" button, signaling the IVA to use the digital certificate on their inserted smart cards to digitally sign their ballots.

The ballots submitted from home, office and polling place will be stored during the voting period on the electoral server. The final results will be known within seconds of the ritual clicking of the "Calculate Totals" icon on the control terminal at the office of the election administrator. No more waiting around all night for concession speeches and for victory parties to begin. Democracy will be on Internet time.

The choice for officials and voters then, is clear. Dare the electronic electoral edge, or be left behind. Give citizens access to voting through the most powerful communications tool ever devised, or see political-participation rates drop so low that any claim to being a democracy will be laughable. Our choice now is reminiscent of and is part of the larger set of choices referred to by the Raymond Massey character at the end of the 1936 film version of H.G. Wells' "Things to Come": "Which shall it be? The universe ... or nothing? Which shall it be?"

Marc Strassman is the executive director of the Campaign for Digital Democracy and the president of The Internet Voting Company.

Could the Internet Change Everything?

Thursday, June 17, 1999

The recent controversies involving racial re-apportionments of congressional districts highlight some of the ways having Internet voting as a mainstream capability might allow us to move way beyond many of our current political dilemmas (and into new ones).

Once we can vote over the Internet, the process of self-governance might begin to take on characteristics not possible with the inflexible, industrial metaphor-based systems we mostly use now, ones that essentially require everyone to (often literally) punch in at the voting factory at one time and in one place.

With the legalization of Internet voting, individual voters will be empowered to vote more or less whenever and from wherever they please, within certain limits. Like telecommuting, televoting as a process is indifferent to how the individual voter performs the voting task (or what they are wearing as they perform it) and is interested only in facilitating the production of the work product, in this case the completed digital ballot.

New affiliation

With Internet voting, and the recent passage of federal legislation allowing states to elect representatives in ways more complex than single-member-winner-take-all constituencies, it may become practical to allow voters to aggregate themselves in new and creative ways. Voters can achieve representation in ways they consider more meaningful than the current geographically-based system.

California recently enacted an open, or "blanket" primary, designed to allow independent voters to vote in the often-determinative primaries of the "major" parties. To a great extent, this reform has rendered completely meaningless the idea of membership in a political party, since non-"members" are now allowed to pick a party's candidates.

Combined with the right to register, or re-register, over the Internet, this arrangement could quickly lead to the proliferation of many new smaller

parties. With the transaction costs of changing your "party affiliation" reduced to almost zero, voters could flow into and out of parties with ease.

These new cyber-parties could appeal to potential members on the basis of race, ethnicity, age, gender, height, income or location. They could also organize themselves around ongoing issues (such as education, crime, health care) or ad hoc concerns as they arise (e.g., stop the bombing, introduce ground troops, negotiate a settlement). These new organizations then could look for new ways to exert traditional political power.

The two-party system as we know it, for better or worse, may therefore be an early victim of Internet voting.

Is direct democracy far-fetched?

Successful Internet-based initiative campaigns (in which digital certificates are used to sign initiative petitions online) in multiple states will focus on substantive issues of interest to voters, while simultaneously building the organizational and technical infrastructure for a national initiative process.

The emergence of an Internet-mediated national initiative process will accelerate the political transformation being effected by Internet voting on the national level. The new state-level, small-party groupings will want to merge with like-minded colleagues into national parties to pursue common agendas through the national initiative process and to help to elect sympathetic representatives in multiple states.

With proliferating state and national electronic initiatives, the need at any level for "representatives" to "represent" voters who have by now repeatedly demonstrated their ability to legislate on their own without the sky falling or civil liberties being trampled may be called into question. Direct digital democracy, the specter haunting the contemporary political landscape, may no longer hesitate to speak its own name.

That same transition to a broadband, ubiquitous, invisible, global Internet that is happening in the United States could take place around the world, at all levels of government. The result could be a global aggregation and merging of like-minded individuals and groups to form global parties, which could pursue "free-trade-with-a-vengeance" or "the-environment-first" agendas, working up and down the jurisdictional ladder worldwide to implement their preferred policies.

Such a politics would eventually undermine the authority of nation states,

which might, under the impact of globalized Internet voting and its offshoots, go the way Italy and France may soon go as a result of the creation of the European Union.

‘We are the law’

As a result, individuals and groups would be free to assert their values and preferences instantaneously and universally. They could appeal to global public opinion, and use sensible thinking, clever sound bites, compelling images and emotional appeals to convince billions of people of their suggested course of action.

Legacy national elites and global corporations might or might not find this state of affairs to their liking. Such groups could be expected to support, oppose, or attempt to co-opt the transformation spelled out here depending on how they felt it would affect their own interests. The dialectic of power between these entrenched elements and the emerging world democratic entity may be the core conflict and the main story of the early 21st century.

Toward the end of "The Verdict," Paul Newman's character tells the jury, "You are the law." We the people are equally sovereign in this democracy, and letting ourselves use the Internet to govern ourselves will position us as the direct descendants and heirs of both the ancient democrats of classical Athens and the Enlightenment democrats of neo-classical colonial America.

As third-wave democrats, using the Net to realize the dreams of our political progenitors, we won't be the last step in social evolution, but we will be taking a quantum leap into a new paradigm that will yield a qualitative increase in our ability to govern ourselves and manage our affairs as a mature, but still vibrant, species should.

Maybe not childhood's end yet, but at least graduation from kindergarten. As Churchill said, "Not the end, or even the beginning of the end, but perhaps the end of the beginning."

Marc Strassman is the Executive Director of the Campaign for Digital Democracy and the President of VoteSite.com, the internet voting company, which can be found at http://www.votesite.com.

Putting the 'E-' in E-democracy

Thursday, September 16, 1999

E-mail is widely recognized to be the most popular of all Internet applications. Likewise, making sure that your legislative representatives know how you feel about issues and how you would like them to vote on specific bills is among the most important of your civic responsibilities. It therefore stands to reason that using e-mail to express your political views to your representatives in the halls of government is one of the most likely points of intersection between the government space and the Internet space.

Yet, e-mail has not evolved into a frictionless means for communicating public sentiment to elected lawmakers for both political and technological reasons. The technical problems now are largely solved or soluble; the political obstacles may take a little longer to remove.

Cleaning out the inbox

Chief among the technical problems is restricting incoming e-mail to a legislator to messages from his or her constituents. Since, apart from his contributors, the media and his conscience, constituents are the most important factors in a representative's political life, he must expend that most precious of commodities, his attention, mainly on them and not on well-meaning people who do not affect his re-election chances.

Fortunately, the same identification and authentication technologies I have been exploring in my efforts to build and implement an Internet voting system easily can be adapted to identify constituents and authenticate their status as bona fide electors in any given representative's district.

In fact, some of this technology is so sophisticated that it is not difficult to allow constituents to choose to authenticate themselves as residents of a particular district while still obscuring their own particular identity. Whether this will make a greater or lesser impact on the target representative is a political, not a technical, issue.

Once e-mails have been filtered/sorted to exclude non-constituents, the next problem is making sense of them. As things stand now, armies of interns in the halls of Congress and other legislative bodies busy

themselves continuously opening paper envelopes and sorting the enclosed correspondence according to whether it favors an action, opposes it, or wants more information about it. Stacks of letters accumulate, and constituent opinion generally is assumed to be analogously expressed in the relative heights of the "pro," "con," and "send me more information" piles.

Fortunately, existing software applications now can easily be modified to automatically sort thousands of e-mails daily. By publicizing (on the Net) sets of keywords that constituents could use to express simple or nuanced views on public issues, legislators can use these advanced filtering engines to essentially poll constituents constantly and in depth at a relatively low cost.

Toward direct democracy

In fact, existing and emerging e-mail systems soon will become so powerful that, assuming we can answer the question of how to provide everyone with equal access to e-mail, the whole political system might soon change. The question may soon arise as to what function, other than negotiating with other representatives, is being performed by a "representative" when the constant flow of e-mail allows a software program to determine precisely the state of public opinion within a district.

If we can determine via authenticated and electronically-sorted e-mail what the percentages are in each district of citizens who are for or against an issue or bill, and we can reach a consensus on how to trade off competing interests, according to the importance of the issue to each voter, the current balance of compromises made in the past, and whatever other obvious or complex factors now guide the deliberations of our representatives then maybe we can let millions of e-mail votes determine the direction of the republic.

Would the results necessarily be any worse than letting the current system, so heavily influenced by campaign contributions from entrenched special interests, carry on indefinitely into the future?

Most telling, this scenario closely resembles the likely consequences of initiating a system of Internet voting, along with the granting of voters, at least in states that use the initiative process, the right to electronically sign initiative petitions over the Net.

The Progressive movement originally deployed the initiative process around the turn of the last century. Recently, as momentum has built to use citizen lawmaking more often and more intensely, countervailing

forces have emerged to limit and curtail it.

Efforts to stifle the initiative process abound. Even absent these attempts, it now costs so much to qualify an initiative for the ballot that only the already well-to-do can afford to qualify, thereby effectively excluding almost everyone from this increasingly important means of making law and policy. We should allow citizens, millions of whom are online everyday, to use the same means of identification and authentication they now use to buy books, trade stocks, participate in auctions, and order music and videos to affix their electronic signature to proposed legislation. This would help right the large and growing imbalance in political influence between common people and the professional political class and its clients who increasingly dominate the initiative process, as they also dominate the normal legislative process.

Disintermediating the intermediaries

The common thread that emerges from a consideration of using e-mail to write your representative and of using electronic signatures to sign initiative petitions online is that the Net can render elected representatives irrelevant . In short, the Net can let us govern ourselves.

If the people can easily and relatively inexpensively make laws by proposing, qualifying and passing initiatives online, is a legislature needed to perform the same function? Consider that a legislature makes decisions by consulting tens of people whose opinions and views are highly privileged at the expense of millions who are de-privileged by this concentration of power.

The other obvious common theme is that the Internet, in both these cases, has the potential to "disintermediate" almost any transactional process as it has already demonstrated in the world of e-commerce. Legislators earn their keep by "intermediating" for their constituents. They collect, perhaps imperfectly, information about them and then exchange that information with other "intermediating" representatives to reach a calculation and a consensus on policy and legislation. The sturm und drang of congressional bickering and deal-making is the flashy costume worn by this process of national-level intermediation.

But the Internet lets all of us share the fun. As we see in the instances of e-mail consultations and electronic initiative signing, the Net is about to become so powerful, so ubiquitous, and so easy to use that every citizen can participate more directly than ever before in the making of the rules by which we govern ourselves.

The transition to a more participatory and direct form of democracy will

not be an easy one, but it will have profound implications for all citizens, current and future. Lawmakers, and everyone who prophesies with his or her laptop, should keep their eyes wide open.

Marc Strassman is the executive director of the Campaign for Digital Democracy and the president of VoteSite.com, the Internet voting company, which can be found at http://www.votesite.com.

I wrote a fourth piece for IntellectualCapital, but it never ran. Here it is now, published for the first time.

Myths and Realities in Internet Voting

January 31, 2000

Now that the prospect of voting over the Internet in real elections from remote terminals has become the subject of serious consideration by politicians and industry leaders, it may be appropriate to address and dispel some of the more egregious and pernicious myths that opponents of the process have conjured up as a means of trying to stop what most commentators now consider to be the inevitable advent of this more advanced means of ascertaining the will of the voting public.

The risk of fraud, and of hacking generally, is usually cited as the worst threat posed to the democratic process by unrestrained voting over the Internet from home and office, hill and dale, and anywhere in between. This worry is followed closely, and in the minds of some Internet voting nay-sayers, is surpassed, by concern about "the digital divide," which refers to the uneven distribution of computing resources and Internet access across the vast and varied American population.

In the case of fraud, the standard used by critics to engender alarm is that of an idealized, flawless system for ensuring the honesty of every voter and the integrity of every ballot cast. Opponents of remote Internet voting endlessly imagine and vigorously lament the villainous scenarios they argue that letting people use the same means for voting that they already use for e-mail, e-commerce and countless other tasks will engender.

The threat and/or actual use of emotional and physical violence against intimates are the imagined cases most frequently cited as reasons for delaying into the far future (if ever) the deployment of Internet voting systems. In the vision of these Internet voting adversaries, letting anyone vote from the comfort and convenience of their home computer is an irresistible invitation to everyone else in their household to withhold their dinner, or their conjugal access, or to threaten to or actually beat them senseless in order to convince them to vote for, say, George W. Bush instead of Al Gore. Or vice versa. Yeah, right.

The fear of unrestrained familial violence as an impediment to remote Internet voting in the home gives way, in the context of the workplace, to equally dire fear of predation by "bosses" so intensely eager to deliver the vote for their chosen candidate that they are completely prepared to violate their workers' moral and legal privacy rights by coercing them to vote the company ticket and, failing to achieve that goal by threatening their cowering workers' jobs or, worse, the loss of their of stock options, by throwing out the real votes cast by employees and substituting their own, more congenial

results. If anything is more absurd than home voting scenario above, it's this workplace one.

Every passionately expressed alarm about the ability of 14-year old hackers to decisively alter election results emerges from a mindset that steadfastly refuses to realize or acknowledge that most, if not all, elections are the culmination of months of campaigning during which participants' polls and media polls constantly monitor the state of voter opinion about the candidates or ballot measures. Anyone who thinks he or she could thwart the will of the voters by somehow artificially altering the election results by hacking into the voting system and posting vote totals that are drastically at odds with the mass of polling data that by that point are part of the public record is almost by definition too stupid to carry out the technical procedures that would be required to do so.

Furthermore, election results today ARE ALREADY collected and processed through computer networks. Merely altering the method by which voters indicate their choices and submit their ballots by letting them vote from their home and office computers, would be a change in degree, not in kind, as far as the overall process for determining election results goes. Ballots are already being counted by computers (in Los Angeles County, on IBM 360s from the '60s) and the totals are being compiled through network systems. If using networks for voting is as dangerous as the critics of Internet voting say it is, why haven't the existing, legacy systems been compromised? And how would bringing zero-something technology into the process make the system more, rather than less, vulnerable?

And now, the digital divide, as it relates to Internet voting.

From the moment the first circuit was completed in the first computer, there has been a digital divide, in that case between the scientists who built the computer and everyone else on the planet. In the early 80s, when cellular phones cost $1200 and needed to be installed in the trunk of your car, there was a cellular phone divide.

While there has always been a digital divide, the term itself seems to have its origins in the Clinton administration's recent efforts to measure, label, and then reduce it. Its emergence as a convenient label for the disproportionate distribution of computing and networking resources, as it applies to various ethnic and income groups, was fortuitous from the point of view of Internet voting's opponents.

Now, in a complaint filed in the United States District Court for the District of Arizona, it is alleged that the use of Internet voting unlawfully discriminates against minority voters because, among other things, "African-American and Hispanic households are only 40% as likely as white households to have home Internet access."

The rules of the Arizona Democratic party's presidential primary in March, which this complaint seeks to enjoin, allows all registered Democrats to vote from computers in their workplaces as well. No mention is made of this fact in the complaint nor is any data

presented concerning the access of minority voters to workplace computers, other than mentioning that participating voters can "vote over the Internet from a remote location."

Apart from the specific dishonesty in this complaint of arguing that the world's first binding public political election should be called off because Internet voting access for minorities is limited, without mentioning or investigating their ability to vote from their workplace, and arguing on the basis of this spurious data that the Democratic Party of Arizona should be prevented from offering Internet voting opportunities to anyone, there is the larger picture, the historical relationship between opponents of Internet voting and the minorities that they claim to be protecting.

As mentioned above, the digital divide has been around for a long time. Where were these defenders of minorities' interests then? For that matter, where are they now when it comes to closing the digital divide? One completely normal response, in fact, the only response possible for people who consistently support equality, non-discrimination, and full and equal access to the democratic process for all, is not to hold back those with Internet access who want to vote over it, but to see to it that ALL Americans, regardless of their race, ethnicity, or income, have access to the Internet and to the computing resources to take full advantage of that access for their educational, personal, commercial, and political needs.

The commercial sector is working hard and creatively to vastly broaden the universe of Internet users. Programs to give potential users free computers and free Internet access (including free DSL access), in exchange for valuable demographic data, are spreading rapidly. Thanks to Moore's Law, the cost of an equivalent amount of computing power continues to drop. The Clinton administration is asking Congress for $100 million to help low-income Americans go online.

Will the opponents of Internet voting who claim it is discriminatory against minorities and the poor put their money and energy into these and other, or their own, efforts to resolve this American dilemma by empowering all our citizens with the essential tools of modern, 21st century American democracy? Or will they focus on crippling those who already have those tools, so that all are equally deprived of democratic electronic participation in shaping their government?

In the answer to this question will be revealed the true measure of the plaintiffs' commitment to the integrity of American democracy.

Chapter 3

Presentations at Public Events

On May 7, 1999, I spoke at a conference in Washington, D.C., organized by the Initiative and Referendum Institute. David Broder of the Washington Post was there and he wrote the following:

David Broder Covers Me at the Initiative and Referendum Institute Conference

From page 237 of David S. Broder's "Democracy Derailed: Initiative Campaigns and the Power of Money":

He was followed by Marc Strassman, the founder and leader of the Campaign for Electronic Democracy, an Internet-based national effort to persuade states to allow electronic voting and—where the initiative process is available—the collection of ballot-measure signatures via the Internet. If the legislatures see the beauty, simplicity, and economy of this scheme, and Congress does the same for the nation, "we can have initiatives, voting, politics, and government at the speed of thought," he said. "What about the people who don't have computers?" a member of the audience asked. "They will get cheaper and smaller," Strassman replied, "and a liberal government would want to give computers away" to those who need them. Some might be skeptical, but Rick Arnold [owner of a signature-gathering company] assured the audience, "Democracy will be changed by this technology." He added with a smile, "I'm looking for another job myself."

Somewhat surprisingly, given his own use of the initiative, Ron Unz said he was skeptical of this vision. "We'd have eighteen hundred initiatives on the ballot in every election in California," he said, "and people would get sick of it, just like they're sick of government-by-polling today. We should raise the barrier, discourage people from putting up initiatives. There should be some kind of merit test." But the proponents were not fazed. "The legitimacy of an idea would be measured by how much support it has," Strassman said.

Published by Harcourt, Inc.

In the fall of 1999, I was invited to participate in a conference on "Frontiers of Internet Politics," which took place at the Ronald Reagan Building and International Trade Center in Washington, DC. Here's a copy of my notes for my remarks at this event on September 16, 1999.

Remarks at the "Frontiers of Internet Politics" Conference

1. Hi

2. Allow me to introduce myself; I'm a man of wealth and taste. I run Campaign for Digital Democracy

3. How many of you would like to be able to vote over the Internet?

4. Since Warren Beatty may be running for President by the end of this month, and the distinction between show business and politics may be even more indistinct than it is now, I thought I would frame my remarks today with references to two films by Frank Capra, a director whose populist sentiments Mr. Beatty professes to share.

5. The first film is that perennial favorite, "It's a Wonderful Life." What I want to borrow from that film is the use of alternative scenarios to make a point. In one sequence, we see what happens to Bedford Falls without the Jimmy Stewart character. Similarly, I'd like you to imagine a scenario in which, over say the next dozen years, the Internet and everything associated with it continues its prodigious expansion and intensification.. But not Internet voting. This scenario implies a population of consumerists ants, reduced to watching Internet television and buying things online. Any vestige of humanity as sentient beings exercising free will will be a faded memory. Compare that to a world in which we get to vote over the Internet and participate frequently in the decisions that affect our lives.

6. Internet voting is simultaneous extremely mundane and extremely subversive.

7. On the one hand, it's no more radical than absentee voting by mail.

8. On the other, it might pave the way to direct digital democracy and the abolition, or at least the eclipse, of representative democracy.

9. Let me give you a very abbreviated history of Internet voting in California, which is pretty much the history of Internet voting everywhere.

10. VVRI, AB44, AB44-2, CIVI

11. Where does CIVI stand? Version 8.x will go to the Attorney General by the end of this month. AG, SOS, back. Online with PDF files.

12. Download, print out, sign or circulate, mail in.

13. Sign it digitally for fun and practice, and on the outside chance we can get them approved.

14. Countering a spate of recent efforts to make it harder to qualify initiatives for the ballot, the Internet voting system will make it easier.

15. Unstated collateral effects of Internet voting legalization:

    a. privatizes important government sector involving direct citizen-state interaction, setting precedent
    b. provides millions of citizens with id and authentication means for future transactions with state and for e-commerce
    c. lowers switching costs for party switching
    d. paves the way for legalization of autonomous smart agents
    e. enables international and global electoral jurisdictions

16. Internet voting addresses the very issues addressed by Shays-Meehan, namely, voter alienation and apathy.

17. If one political party enthusiastically and effectively embraces the idea of Internet voting and works to achieve it, this party may experience a great upsurge in support when it comes to pass, and parties who opposed it suffer a similar decrease.

18. What I was thinking, when I stood outside the health food store in 1996 collecting signatures on the Virtual Voting Rights Initiative, what I thought when I testified before a committee of the California State Senate in 1997 on behalf of the doomed AB44…is what I think now—is that this is our country and our government and if we want to use the most modern and most effective means of governing ourselves, well, then we can. I hope you join me in the effort to assure that we can.

19. The Greek revival architecture that graces this fair city has an implicit meaning, that America is the heir of classical Greece, that American power and technology, married to the Greek esthetic and the Greek ideal of democracy, can create a modern state and society that is both great and good. That is the implicit meaning of Internet voting as well, that combining technological capability with a good idea can result in the creation of a powerful tool for human self-empowerment and self-governance. Just as this city reflects and

expresses this combination, so does the idea of Internet voting. As we admire and work within the first, we should being to contemplate how we can update this benevolent combination with another joining of power and ideal.

20. Let's close with a visit to another world created by Frank Capra, the world of "Mr. Smith Goes to Washington." Like the Jimmy Stewart character, I visited the Lincoln Memorial, on Tuesday night, although I had no Jean Arthur to show it to me. I wasn't able to get onto the Senate floor, real or celluloid. But I do remember the scene set there, where Jimmy Stewart is waiting for the mail to arrive to overturn the plans of the cabal. When it arrives, the day is saved, at least temporarily. It's the mail that does it, bushels and bushels of mail from Americans exercising their rights and expressing their opinion.

Internet voting is like those bushels of mail that saved the day for Jimmy Stewart and all of us. It will let us tell our government representatives what we think of the policies they want to adopt on our behalf. It will keep in "demos" in democracy. But letting ourselves use the Internet to do this will make it easier, faster, more effective It's our country now as it was our country then as it has been our country from it's very beginnings, if not before. We ought to hesitate no longer to make sure we have the best possible tools to determine and carry out our will, as a free people. To me, that means Internet voting.

Vote where you live—use the Internet.

-30-

While not strictly speaking an event dealing with Internet voting, the Special Meeting of the Information Technology and General Se3rvices Committee of the Los Angeles City Council held on November 3, 1999, was nevertheless an occasion when issues involving how decisions are made about providing citizens with access to systems potentially of use in politics ought to have been raised. I tried to raise them in these remarks.

Remarks on Open Access

November 3, 1999

Members of the City Council, staff, media, and the public,

My name is Marc Strassman. I live in Valley Village, just down the road.

I'm the President of e-topia, a content origination company that produces audio and video clips for distribution over the Internet. In order for me to do my work, it's essential that I have a broadband connection to the Internet. It's also essential to me as a creator and distributor of digital content that as many other people as possible also have access to broadband connectivity, so that they can listen to and watch my programming at the highest possible resolution, the most frames per second on their screens, and the highest quality of sound, capabilities that require a wide, fast, broad pipeline into the Internet backbone.

I get my broadband connection from Pacific Bell and PacificNet in Universal City. I pay Pacific Bell $39.00/month to provide the DSL line and I pay PacificNet $10/month to manage my connection to the Internet.

I believe that the principal reason I've been able to get a guaranteed 384kps Asynchronous Digital Subscriber Line from Pacific Bell for $49.00/month is because its parent company, SBC, felt threatened enough by the POSSIBLE competition in broadband from cable companies to drastically lower their prices for this service and to roll it out much faster than they had originally planned.

It works fine and it greatly improves my use and enjoyment of the Internet.

Let me repeat what I said: it was the threat of competition from the cable companies that made it possible for me to get good service at a reasonable price from the phone company.

Now the phone companies and AOL, under the banner of what they have chosen to call "The Open Access Coalition," a pseudo-grass roots organization modeled, it seems, on the smokers' organization similarly organized by Philip Morris, want you to give their multi-billon-dollar organizations a break and allow them to share the use of the investments that cable companies have made, are making, and might make, in building broadband capability into their system.

The reason they're spending so much time, energy, and money to make the case for "Open Access" is because they see fully-wired cable companies as a serious threat to their existing almost-monopolies in telephone service. They believe that if they can convince enough public officials to force their competitors to give them a virtual free ride on the back of the cable plant required for delivering broadband services, then cable companies will think twice, or more, before making the serious investments that can give the powerful, consolidating, almost-monopoly phone companies a run for their money.

They also believe that if they can just tie the whole process up long enough with appeals to city councils, appeals to Federal courts, and appeals from some imagined injustice they are claiming they'll suffer, then this will also be enough to dissuade cable companies from bothering to build out their broadband capability.

If this happens, or more to the point, doesn't happen, then they can **retain** their monopolies on voice telephone service. Then they can **raise** their own broadband DSL prices. Then the competition that is essential for lowering prices and increasing the availability of broadband will be gone and every business, every consumer, every government, and every citizen will be worse off because of that.

On a related note, as of yesterday, both the cities of San Francisco and Santa Monica had enacted local ordinances prohibiting certain ATM charges. The banks, of course, have said they'll oppose these measures in court. On the same issue we're discussing here tonight, forced access to cable plants, the City of Portland has voted to support "open access". This has, of course, also led to an on-going legal case. All these efforts in regard to ATM access and broadband access by organizations of autonomous local citizens or local citizens organized and supported by giant outside corporations, against mega-corporations with strong local presences (Think globally, market locally.) highlight what will no doubt be a frequent occurrence in 21st century America, disputes and debates about both the substance of electronic access issues and the authority of citizens within political subdivisions to enforce their will on commercial entities, or other governments, that are regional, national, or global in their reach.

Beyond the substance of this issue being discussed here tonight is the meta-issue of determining the relative authority of linked jurisdictions. The effort to reach consensus on this procedural, meta-issue will no doubt be complex and it may be divisive. After all, a similar dispute, the substance of which was slavery, and the procedural form of which was "states rights," led to a certain protracted dispute-resolution process far more extensive and far bloodier than any we can expect to see emerge from our discussions here tonight about how we're going to get our broadband Internet connections.

In this particular situation, though, where the Federal Communications Commission is strongly in favor of doing nothing at this time, we in the City of Los Angeles, and you as our elected representatives, will do the least harm and the most good if we follow their lead and choose to do nothing as well, letting the free market in services, protected by what we have here, a free market in ideas, run its course. That way, the most broadband

service can reach the greatest number of people, and we will be that much better able to use the Internet as a conduit and forum for the ideas and expressions we must rely on to sort out future, and even more complex, issues involving our livelihoods and our freedom.

Thank you.

By the fall of 2000, I was working to qualify the Smart Initiatives Initiative, legislation to provide every Californian with a digital certificate, a smart card, and the right to use them to sign initiative and other official petitions online. My inquiries to the PKI Forum about digital certificates and related subjects earned me an invitation to address their Fall Conference in Montreal, Quebec, Canada. Below is a copy of my remarks, as originally prepared, and also a print-out of the PowerPoint presentation I eventually used instead. To hear the actual delivery of this material, go to:

..\Montreal PKI Forum\PKI Forum audio\PKIForum.rm

Toward a Ubiquitous E-Democracy Powered by a Universal PKI

At the risk of belaboring the obvious, let me remind us that the Internet has created a global system for the disintermediation of any process consisting of the transfer of information from person to person, organization to organization, or person to organization. And vice versa.

This means that any existing process involving the generation, collection, sorting, analysis, or distribution of information is subject to new dynamics, new cost structures, and the elimination of no-longer-needed individuals and organizations. Naturally, these unneeded entities resist their own demise. Nevertheless, a set of other people and other organizations, centering their operations in and over and around the Internet is emerging in every significant sector of life and work to challenge the hegemony of existing forms and working day-by-day to replace them with cheaper, faster, more accurate, more broadly inclusive ways of doing things.

Sometimes these new ways of doing things are explicitly illegal under existing law. Napster and the controversy surrounding it are an extremely good example of this. Millions of Napster users have used this system of peer-to-peer file exchange in order to augment their MP3 collections at no additional charge beyond whatever it costs them to access the World Wide Web. The Recording Industry Association of America, finding free music that doesn't pay them anything intolerable, took Napster to court, won, then saw the judge grant the program a stay until an appeals court can consider the case.

Let me briefly cite another case where the Internet was on the brink of undermining the entire election system of the US and, indeed, any country on earth, and where lawyers made it clear that such activity would not be tolerated. A number of citizens, fed up with the fact that, in their opinion, elected representatives routinely received money for their legislative votes, mainly in the form of campaign contributions from parties with business before their bodies, decided that what was good enough for the legislator/goose should be good enough for the citizen/gander and put their votes up for auction to the highest bidder on eBay.

This move was praised by many as inspired street theater, but denounced harshly and authoritatively by election officials who sternly reminded these would-be vote sellers that what they were attempting to do was totally and completely illegal, and that they would be fined and/or imprisoned if they persisted in their errant ways. As far as I know, the "sell-your-vote online" movement died a'borning, under the legal onslaught unleashed against it by the protectors of the public vote.

This incident, by the way, provided piquant evidence of how fed-up with "representative" democracy many American citizens are and how, when they feel the need to do something about their frustration, it's the Internet they turn to. As we'll see later, there is a solution to this problem of citizen anger and apathy lurking in the Internet, and it's completely legal

In both the Napster and vote-selling cases, the fundamental qualities of the Internet (its emerging near-ubiquity), its speed, low cost, adaptability to change, its ability to transfer vast amounts of information [when more and more of what there is is being recognized as fundamentally information] to millions of users worldwide almost instantaneously meant that like-minded, or complementary-minded, people could create a free market for exchanging commodities, in these cases MP3 files and votes.

Only the guardians of the music and the guardians of the votes stepped in, saying, "We own the music, and we control the voting process. Copyright infringement and vote tampering are serious crimes. You will do it our way or we will severely punish you. We shall be obeyed."

So far, the resolution of these conflicts is still up in the air, with vote selling apparently a dead letter right now, and Napster waiting further judicial rulings. But even if Napster is shut down and the code scattered to the four winds, there are other, harder to pin-down, applications that can duplicate its functionality. And as for vote selling, when Internet voting becomes ubiquitous and access to your ballot from any Internet connection through the use of a centrally-stored digital certificate by invocation of an easy-to-remember password becomes the key the electoral door, who can doubt that someone will create a market for the transfer of these passwords in exchange for money from individuals and organizations who have more money than they have votes?

This is not an argument in favor of abolishing Internet voting, but it is a cautionary observation that ought to inform our thinking about what the Internet can do and what it should be allowed to do.

One thing that I think it ought to be allowed to do is collect bona fide signatures from citizens who are willing to digitally sign initiative, referendum, and recall petitions online. The current initiative petitioning process is arcane in the extreme, costly, slow, prone to errors, and it cries out for some of the functionality that the Internet can bring to the automation of any process involving the manipulation of information.

The petitioning process, now with pen and paper, soon I hope with mouse and keyboard, is purely an information activity, and therefore ideal for being moved into cyberspace. Proponents formulate the idea, find language for it, work with others to edit and craft the proposed law. Officials receive documents, review them, certify them for timeliness and adherence to proper form and return them to the circulators. So far, this process hasn't cost too much.

Then the process of collecting the signatures begins. In California, 420,260 signatures need to be collected to put an initiative proposal on the ballot. That's 420,262 valid signatures. It's usual to collect many more than that, due to all manner of potential irregularities, including unreported changes of address, missing or incorrect information, illegible data, and so on. The going rate to hire a competent signature gathering company to collect the necessary signatures in California today is one million dollars.

And the problem is not all in the cost. Because it would be prohibitively expense to laboriously hand check all 420,260 pen-and-paper signatures, election officials make it only moderately prohibitively expense by using arcane formulas to randomly sample the inky scratchings on bleached dead trees that they've received by the heaping boxful, usually on the last possible day allowed by law.

This means that clerks must manually compare the small percentage of signatures actually being checked against the signature submitted by the voter when he or she originally registered to vote. I understand that they use quite modern scanning and screen projection methods to do these checks, but I somehow always imagine a lot of in-line skaters scurrying around a large concrete warehouse when I think about how the signatures are validated under the current system.

It was suggested, back in times when the implicit sexism of the stereotype was allowable, that if the telephone company (there was only one then) couldn't depend on new advances in telecommunications technology to handle the rapid increase in call volume, then it would take every woman in the United States working as an operator to accomplish the same amount of switching.

If we wanted the same performance out of our deregulated, multi-national, integrated data-and-voice networks today, and wanted to do it with humans, we couldn't do it at all, both because there wouldn't be enough of them and because they would not be capable of the fast, sophisticated data transformations which computers and networks are able to perform.

If we relied solely on human (mostly women, ironically) agents to process the manual signatures now used to qualify initiatives for the ballot, we'd end up with a process that is expensive, tedious, error-prone, and rag-tag. Wait a minute. That IS what we have.

But digital signature technology, which your companies have pioneered, established, and grown, could do away with all of these antiquated anachronisms. Instead

of standing in the rain, being chased away by angry store owners, postal employees, and dogs, petition circulators could stay indoors or even vacation in Canada if they liked. Citizens, instead of being barraged by entreaties to sign petitions they've never heard about, don't understand, and don't care about, or brow-beaten by overzealous circulators, or frustrated because they are being asked to consider an issue and a resolution of it that may be of great moment when they are already a half-hour behind their hectic schedule, could read, study, and contemplate these proposed laws for as long as they liked from the comfort of their home or office (not on company time, of course).

They could access supporting materials, listen to or read opposing views, chat with others interested in the issue. Then, if they decided they wanted to put the measure up for a vote of the people, they would go to the proper page, invoked their stored digital certificate through the use of their unique, private, inviolate password, and digitally sign the petition.

[It's often said that what we call "e-mail" will soon just be called "mail," and what we call "e-commerce" will soon be called just "commerce." When Smart Initiatives come into general use, they will certainly speed the arrival of the day when what we now call "digitally signing" will be called "signing."]

Of course the advantages inherent in the digital signing of official petitions do not accrue only to their circulators and signers. They also ensue for the election officials formerly mired in the plethora of paper constituted by all those flat dead trees with ink markings on them. Now, instead of checking a small percentage of signatures, they can check all of them. Instead of relying on human eyesight and memory to encode and decode images and parts of images, fast, accurate, powerful servers will do all the encoding and decoding needed to determine the validity of the digital signatures. Valid digital signatures on the petition will be counted towards the required total. Invalid ones will be rejected. Totals will be calculated at the speed of thought. No fuss, no muss, no bother.

It's not just the telephone system that couldn't be run at its current level without computers and networks. It's just about every activity we encounter in our daily lives, including, among others, airlines, hospitals, public safety, telecommunications, national defense, the provisioning of food, the operation of our power grids. You get the picture. But there is one sector where computers and networks do not yet hold sway, and that is the elections sector.

The two domains that are linked by elections, politics and government, have been moving rapidly to adopt new technologies to better and more cost-effectively carry out their respective missions, namely electing candidates and administering bureaucracies. But the crucial connection between politics and government in a democracy, the elections by which the citizenry makes its choices between alternative candidates or propositions, has remained remarkably immune to the wildfire of "creative destruction" that the Internet has unleashed across the economy, society, and culture.

The reason for this technological lag is not technological, but political. The initiative process, frequently the agent of changes that are controversial, disruptive, or strongly-resisted, and that often involve the re-distribution of political power, are not much appreciated by the powers-that-be, especially elected representatives, and, sometimes, judges. Recent years have witnessed, and this year continues to witness, concerted efforts by political incumbents to limit and weaken the initiative process.

Things apparently got so bad that David Broder, universally-acclaimed as America's foremost political reporter, thought it necessary to write a book, called "Democracy Derailed," in which he railed against the initiative process as a tool for self-indulgent rich guys bent on having a little fun by spending a lot of money to persuade people to support their nefarious schemes. The book was not well-reasoned, in my judgment, but it was a bell-weather reflection of the fear held by many incumbents (in this case the incumbent "America's foremost political reporter") that letting ordinary people propose and vote on the laws and spending priorities they want their government to enforce and implement, respectively, is extremely inadvisable and had best be brought to heel, if not eliminated, as soon as possible, in order to preserve both democracy and the republic.

I disagree with David Broder on this. While the disproportionate influence of a few rich people in politics and government ought to be guarded against wherever it arises (and Broder, surprisingly, has nothing to say about the disproportionate influence of a few rich people wielded through the "campaign financing" system), the initiative process is remarkable in that it often provides the only means by which ideas and groups excluded from power can have an impact. Whether from the right or from the left, or any part of our new, multi-dimensional political spectrum, individuals and organizations with innovative ideas, fresh perspectives, or long-standing grievances can use the initiative process to bring their issues into the mainstream, have them subjected to discussion and debate, and offer them to their fellow citizens as a way of moving forward on the issue.

So I want to say that not only is the digital signing of initiative petitions a cost-effective, elegant, energy-efficient, and generally cool way of qualifying initiatives for the ballot, but the ease and cost-effectiveness that it will provide to initiative circulators will serve as a countervailing force against the growing crescendo of voices calling for higher signature counts and more restrictions on the rights of physical circulators.

Having made the case for the use of digital certificate technology as the preferred means of signing initiative petitions, I'd like to say something about actually converting this proposal into policy.

Ideally, the several state legislatures would immediately understand the value of these suggested technopolitical reforms, and enact them forthwith. Practically speaking, this is not going to happen, for two primary reasons. First, although it's improving, the general level of technical understanding among state legislatures is not yet in sync with the rapidly evolving Internet landscape. And second, no one likes to give up power, and

state representatives are no exception. Making it easier for the people in their constituencies to make the laws under which they live would undermine their authority, their power, and their ability to collect "campaign contributions" from special interests. So the path to ubiquitous e-democracy through a universal PKI does not run through the state legislatures.

However, more than 20 states have the initiative process, established a century ago precisely to circumvent the recalcitrance of legislatures in thrall to that era's special interests. By laboriously and expensively collecting voter signatures on petition forms, it would be possible to place initiatives on the ballots in order to reform existing government procedures and replace them with a more popular and a more technologically-advanced alternative.

This is what I set out to do by creating the Smart Initiatives Project.

In the era of smart cards, smart roads, and smart bombs, I figured that the political system could use its own smartness upgrade. So, as I outlined earlier, Smart Initiatives would put the power of the Internet and PKI at the service of political reform, and allow governments to leverage technology to improve the responsiveness of the democratic process.

Right now, I'm concentrating my efforts on creating a Smart Initiative law for California. Having drafted a conceptual version of the proposal earlier this year, I collected the requisite voter signatures on it at UCLA, sent the draft to the Office of Legislative Counsel in Sacramento (the same group that writes laws for legislators and their committees), and a few short months later, got a nicely-written, legalistically-phrased document which is now called the Smart Initiatives Initiative.

It's kind of a boot-strapping operation, using the old initiative process to bring in the new one. As you can tell from its name, it is a proposal that seeks to change the very way such proposals are handled in the future. It is an attempt to use the tools of reform as they now exist to transform them into something more powerful, more useful, more capable of easy upgrades as politics and technology evolve. But it is a reform that, unfortunately, needs to employ the existing archaic, inefficient and expensive methods it would at least partially replace in order to reach the ballot and be considered by the voters of California.

It costs one million dollars to qualify a ballot initiative in California. If the Smart Initiatives project can raise that much money in a timely manner, the Smart Initiatives Initiative will go before the voters of California, probably in the spring of 2002. If it passes, the State of California will be required to establish itself as mega-Certificate Authority, and to provide every adult in California with a digital certificate on a smart card and also make the certificate accessible, through passwords known only to its user, from any suitable electronic device.

Now isn't that something every one of you here today would like to see happen?

The Smart Initiatives Project is also working to launch similar efforts in a number of other states with the initiative process, including Washington State, Oregon, Arizona, and Massachusetts. Qualifying a Smart Initiatives Initiative in these states is considerably less expensive than doing it in mega-state California. Given sufficient funding, it would be possible to bring Smart Initiative campaigns to over twenty states, and, if it passed, to have all those states be required to set up this same kind of CA and distribute millions more certificates to their citizens.

For better or worse, it all comes down to money. I've thought this up, written it, submitted it, pursued it, because I believe that democracy and every citizen would benefit from having the right to use Smart Initiatives. But I don't have one million dollars. As much as this effort is designed to replace existing ways of doing political business, the fact remains that we still have to do business the old-fashioned way in order to create the opportunity to do business in a new-fashioned way.

That means we have to operate within the constraints of contemporary political rules, the most important of which is, "you get what you pay for." Everyday, special interests pursue their corporate goals by financing candidates, especially incumbents, who are in accord with their views and who tend to look favorably upon the expenditure of public monies for the products of the aforementioned company or who favor a hands-off regulatory approach to that company's industry.

The situation is no different here with the Smart Initiatives Initiative. Either the companies that stand to reap a considerable benefit from its passage support it, or else it will not succeed. I've identified three classes of company that I think will most benefit from the Smart Initiatives plan:

1. PKI suppliers
2. smart card companies
3. electronic services companies (insurance, HMOs, banks)

PKI vendors will benefit in several ways from the passage of Smart Initiatives. First, Smart Initiative states would need to buy expertise, software, hardware, training, and so on from PKI and related vendors. Second, the deployment of such large numbers of certificates would mean an overnight leap to almost ubiquitous distribution in Smart Initiative states, and, through the principle of network externalities, thus making everyone's digital cert now even more useful, since so many others would have them, too. This would allow secure authentication to become a commonplace aspect of online transactions and both facilitate and enhance the centrality of PKI in e-commerce and related areas. Third, by upgrading the PKI and the political process in the states which are early adopters of Smart Initiatives, these jurisdictions will become models for others, thereby spurring further deployment in areas that fear being left behind, in some cases even by administrative order or legislative action.

That's if the Smart Initiatives Initiative qualifies for the ballot, in one or more states. But even if it only qualifies for the ballot, and we go ahead with a campaign to pass it, the earned news coverage that such a measure would generate would, it seems to me, be worth much more than could ever be gained by the expenditure of a comparable amount of money in any public relations or advertising campaign.

Digital certificates and PKI are not on most Americans' radar screens. They might not be on most of their screens even after a hearty campaign about them. But many more opinion leaders, company presidents, government agencies, news organizations, and members of the general public would know what a digital certificate is and maybe even how it works, and especially what it's good for, after a campaign to pass a Smart Initiatives Initiative came to their state.

So I think that if Smart Initiatives passed, they would be tremendous boon for the PKI community. If they failed to pass, but managed to educate and inform people about the value of PKI, they would still have earned their keep and done a lot to further the effort to make such tools ubiquitous.

I've been thinking about the relationship between technology and politics for almost a quarter century, since I was a special correspondent covering science and politics stories at **The Stanford Daily**. I would report stories involving the intersection of various technologies and the political process, mostly controversial subjects like swine flu inoculations, nuclear power, and recombinant DNA. I noticed that, with the exception of Dr Edward Teller on the subject of nuclear weapons, neither the political actors nor the technologists seemed to understand the others' fields. And yet the core of the controversy usually involved how to make an informed political decision involving some bit of scientific procedure or data, which was itself often being contentiously argued over. So the situations could get complex.

Around that time I decided that I could do myself and everyone else some good by trying to bridge the gap between technology and politics, by combining a journalist's respect for the truth and skills at ferreting it out and publicizing it, with a teacher's vocation of educating people about facts, demolishing myths, and helping anyone who cared to to gain the knowledge necessary to make the most informed decisions possible.

I did that by running for Congress in 1980 on a platform of "Compute, Don't Commute." From what I understand traffic is like now on the Central Expressway, this may have been one of my most perceptive suggestions. I did it when, in the mid-80s, I co-founded the Cable Communications Cooperative of Palo Alto, Inc., an eventually abortive attempt to put a community in charge of its own telecommunications system. I did it when I wrote the Virtual Voting Rights Initiative in 1996 and the California Internet Voting Initiative in 1999, the first of which mandated the same Smart Initiative system I'm advocating today.

And I'm doing it now by proposing and working to pass the Smart Initiatives Initiative, because I believe it will empower all of us to use technology in a directly political way, and give us as citizens the same effectiveness that we have as Napster users. In the case of Smart Initiatives, that means to have the power to choose our laws as easily (but perhaps with more in-depth consideration) as we choose our tunes.

The difference that technology is making in our daily lives and the changes it is bringing to the world are enormous. Its potential to facilitate our liberation or our enslavement is equally huge. Unless we want to be mere consumers, engulfed and devoured by an all-powerful, all encompassing entertainment/telecommunications monolith, that sees us as commodities, as "eyeballs" to be mesmerized and wallets to be plundered, then we need to do something serious now to increase the power of individuals and groups to exert some control over our own destinies.

Fortunately, we have all the tools we need to do that. We have a Constitution and over 200 years experience using it, making us the market leader in continuous years of democratic self-rule. And we have the technological tools we need to maintain and expand the practice of our democratic rights.

What we still lack, however, is a commitment to putting our high tech tools to work in the service of our highly valued democratic principles, a commitment to applying them in a way that counts, and is not merely an advisory poll. If the states adopt the Smart Initiative idea, they will, in the medium and long run, save themselves money, enable themselves to deliver e-government services on an unprecedented scale, spur e-commerce, and, not incidentally, create the infrastructure for a digital democracy that can and will synergize the complementary strengths of democratic safeguards and network-based computing. Put another way, Smart Initiatives stands for "political reform through Internet power." Properly and adequately financed, it seems to me a powerful, even unbeatable, combination.

Victor Hugo famously wrote that "nothing in the world is as powerful as an idea whose time has come." The idea of Smart Initiatives meshes multiple themes in networked computing and our political practice. It enhances the political space, the computing space, and the commercial space. Its adoption everywhere will be good for PKI community. Perhaps Smart Initiatives is an idea whose time has come.

Thank you.

Toward a Ubiquitous E-Democracy Powered by a Universal PKI

(PowerPoint version)

Political Reform through Internet Power

Internet disintermediates information processes.

- **Some information processing organizations adopt Internet faster than others**

- **Government entities are uniquely positioned to accept public efforts to upgrade their capabilities**

The fate of spontaneous popular disintermediation:

- The eBay vote selling incident demonstrates citizen disenchantment with the political process.
- Napster and eBay have demonstrated the power of popular movements using the Internet to disintermediate transaction streams.
- Authority steps in to quell the digital civil disturbance.
- Where will it break out next?
- It's broken out between the MPAA and HRRC.

Let’s use the Internet to sign initiative petitions.

Initiative petition signing is fundamentally an information processing activity.

California petitions need 419,260 signatures. To qualify one costs $1,000,000

Digital authentication of every petition signature is superior to the manual authentication of a random sample of signatures.
Without computers, we’d get nothing done.

We’d be in rough shape if we weren’t running processes with computers.

In the area of petitions, we are in rough shape

Digital signature technology could fix things up.

Having petitions signed online would help proponents, signers, and election officials.

“e-signing” will soon be “signing.”

The Smart Initiatives Initiative will give every adult Californian:

- the right and the means to sign initiative and other official petitions online
- with binding legal effect
- using free digital certificates
- issued by the State of California.
- This is "Political Reform through Internet Power."

Elections link politics and government and need to be automated.

Many sectors benefit from using networked computers, but not election bureaus.

Incumbents are delaying the transition to a modern, rational system.

David Broder doesn't like initiatives.

I disagree with Broder, who doesn't discuss "campaign contributions."

Smart Initiatives will neutralize the growing efforts to suppress initiatives

It would be great to get state legislatures to approve Smart Initiatives, but it's not likely.

The initiative process is really the only way to upgrade the initiative process.

Smart cards, smart roads, now Smart Initiatives.

I created the Smart Initiatives Project and the Smart Initiatives Initiative to bring Internet power to political reform.

Smart Initiatives bootstraps itself from the pre-smart initiatives platform.

California will cost $1,000,000

Smart Initiatives could be qualified in **all** initiative states for $3,000,000

24 states have the initiative process in place today

Their total population is 131,192,000

Source: U.S. Census Bureau, Administrative and Customer Services Division,
Statistical Compendia Branch,
Last Revised: December 30 1999

Money matters.

Same as it ever was.

Three classes of beneficiaries:

- **Public Key Infrastructure providers**
- **Smart card providers**
- **Electronic services providers**

How Smart Initiatives benefit PKI providers: (1)

- Smart Initiative states will need to buy PKI products and services

- Smart Initiative states will raise the bar for other states, who may upgrade to remain competitive
- Millions of additional PKI users will create beneficial network externalities, increasing demand

How Smart Initiatives benefit PKI providers: (2)

- Smart Initiatives put PKI at the center of the e-government discussion, enhancing its credibility as a public sector solution
- Smart Initiatives will mainstream PKI

Even a losing campaign will do wonders for PKI's visibility. PKI is known now only to a select few. After Smart Initiatives, many more will know about it and want to use it in their personal lives, businesses, and in government.

Supporting SI is a win-win.

Qualify and win: get more business.

Qualify and lose: get invaluable visibility.

Previous efforts of mine to upgrade civic life through technology

- Writing for The Stanford Daily (1976)
- Running for Congress on "Compute, don't commute" platform (1980)
- Co-founding the Palo Alto Cable Coop (1982)
- Writing the Virtual Voting Rights Initiative (1996)
- Writing the California Internet Voting Initiative (1999)

What I'm doing now:

The Smart Initiatives Project is how I am currently trying to synergize the democratic process and the best of the new digital technologies.

Technology will bring big changes.

Universal PKI brought about through Smart Initiatives will help keep these changes positive.

We have the tools at hand.
Our democratic constitutions and the Internet, a great combination.

We must commit ourselves to establishing Smart Initiatives everywhere.
Political Reform Through Internet Power
There is nothing on earth more powerful than an idea whose time has come.
--Victor Hugo
For more information or to contact the Smart Initiatives Project, go to:
http://www.smartinitiatives.org
For a copy of this PowerPoint slideshow, e-mail requests to:
info@smartinitiatives.org
To contact me, send e-mail to:
xd@smartinitiatives.org

Chapter 4

Fifteen Easy Pieces

Starting in the summer of 2000, I began writing articles focusing on the need to provide all citizens with digital certificates, so that they could unambiguously and authoritatively represent themselves online in a variety of political and commercial transactions, especially the signing of initiative petitions.

Why a Campaign for the Universal Distribution of Digital Certificates Makes Sense

August 7, 2000

Now arising is a proposal to require each state, through its Departments of Motor Vehicles, Information Technology, and Elections, and working with private companies, to issue to each of its citizens a high-level digital certificate, one that will allow its holder to identify themselves and be authenticated unambiguously and legally over the Internet.

Why this is a good idea:

1. Digital certificated citizens (DCCs) will be able to do business with government at all levels in a less expensive, more convenient, and more secure way than they now can off-line
2. DCCs could register to vote, sign official petitions, and vote online, increasing civic participation while drastically lowering government costs
3. General e-commerce, and m-commerce (mobile commerce) will be enabled much more extensively than at present, growing the economy, and generating new government revenues
4. These certificates could be used to remotely sign contracts, non-disclosure agreements, and other business documents, thereby speeding up and increasing the security of such transactions, while simultaneously lowering costs to all parties involved.
4. The Federal Trade Commission has recently proposed that Congress require all websites to adopt a privacy policy that includes the right of consumers to access data about them in the site's databases. It has been objected that sites would then have to cope with requests for consumer data from sources other than the real customer. Providing everyone with a digital certificate would solve this problem, removing it as an obstacle to the implementation of an equitable privacy policy, thereby enhancing the privacy status of millions of Internet users.
5. If everyone had a digital certificate they could use to unambiguously identify themselves online under a regime of non-repudiation, then it would be possible to build and operate a system that would require campaign contributions over a certain size (say, $100) to be made/reported online with features that would "vet" proposed contributions before they were made in order to exclude any contributions that are illegal according to the operative laws of any time and jurisdiction, taking into account the identify and previous contributions of each potential contributor.

Why this hasn't been done until now:

1. **The Chicken and Egg Problem.** Digital certificates, in spite of their usefulness in identifying and authenticating individuals over the Net, are not yet widely used. One major reason for that can be found in the Chicken-and-Egg syndrome. Not many consumers bother to get digital certificates because not many merchants, either on- or off-line, offer them anything for using them or even allow them to. Off-line, the expense of providing the smart card readers that could accept digital certificates has prevented most merchants from acquiring this equipment, along with the fact that few customers express interest or present such smart cards. For their part, customers, operating in an environment where few merchants have smart-card readers, reasonably conclude there is no point in acquiring digital certificates or smart cards.

   Now, either everyone, acting rationally, has failed to adopt smart cards and digital certificates because there are no good reasons why they should, or the market only needs to be catalyzed by the government issuing millions of digital certificates on smart cards, after which merchants will install the readers and citizen/consumers will use the cards and everyone will benefit from lower costs, more convenience, and greater security. We'll only know which it is if we experiment with it in a market/state big enough to show us which hypothesis is correct.

2. **The Black Helicopter Problem.** Civil libertarians constantly worry that once everyone is registered with a unique, unambiguous number, a nameless agency will begin abducting, or harassing, or imprisoning everyone, starting with them. They ignore the fact that government agencies and many private organization already have more than enough information to do this if they wanted to and weren't constrained from doing so by law, morality, custom, the media, and inertia. Giving people the ability to identify and authenticate themselves in transactions with banks, schools, hospitals, the government, and each other is not going to significantly increase the probability for individual or collective repression. In fact, by opening up the government process online, significant progress could be made towards creating a more inclusive, more responsive government, one much less likely to engage in the worrisome behaviors that some worry about.

What can be done?

If all goes well, in November, 2001, California voters will have a chance to vote on the Digital ID Initiative (DIDI), which will require the State of California to provide all its citizens with digital certificates, at no additional cost to them (except as taxpayers). It will also give them the right to use these certificates to digitally sign online initiative petitions.

Once legislatures in other states hear about this proposal, it's natural to assume that its reasonableness and significant benefits will persuade a number of forward-looking

legislators to adopt it as their own and pursue its swift passage in their own state legislature.

In the meantime, organizations and individuals who see the benefits of the universal distribution of digital certificates can spread the word about it. Getting this infrastructure of "remote assent" in place as soon as possible will mean we can rapidly move on to putting it to use in countless ways to improve our governance, our commercial business, and our lives generally.

This piece first appeared on an early version of the Smart Initiatives website, to explain what Smart Initiatives are and why they're a good idea.

The Smart Initiatives Prospectus

August 14, 2000

As brick-and-mortar government evolves into e-government, giving citizens access to information and services online, it is essential for the maintenance of democracy that these same citizens gain equally free access to making government policy, as well as being recipients of it.

Giving actions taken over the Internet the force of law while giving every citizen adequate authenticated access to the Internet makes it possible to re-form democracy on a basis that is simultaneously both intimate and national, and even possibly global.

Approximately half the states already have in place the initiative process, whereby citizens or groups can propose laws that the state legislature sees fit, for whatever reason, not to pass. But it is difficult and expensive to qualify an initiative for the ballot. In California, it takes at least one million dollars to pay a professional signature gathering company to collect the 420,260 signatures necessary to qualify a ballot initiative.

This means that only either very motivated grass-roots organizations or people or groups with a lot of money can avail themselves of this procedure.

But if it were legal to sign initiative petitions right online, using digital certificates, then a good idea might be enough to propel an initiative onto the ballot. A replica of the official petition form, instead of being presented to harried pedestrians in malls where the owners have done everything they can to exclude signature gatherers and where they continue to object to the presence of citizens who might distract consumers, could be posted on a web site, surrounded by materials explaining the measure and exhorting citizens to sign it.

With the widespread privatization of public space, it is increasingly hard to find places where signatures can be gathered on petitions. Many state legislatures, jealous of citizens making laws they won't, worried that the Internet will disintermediate them the way it's rendered obsolete so many other twentieth century institutions, have tried to limit citizens' rights to collect signatures in public, while simultaneously ignoring calls to put the Internet to work in ways that would circumvent many current real-world obstacles to signature gathering.

Now comes the Smart Initiatives movement, seeking to add petition signing to the growing number of processes that are now being done faster, cheaper, and more conveniently over the Net. The Smart Initiatives Initiative, now pending in the Attorney General of California's office, would let initiative proponents put their measures into

proper graphic form, then post them on the Net, where those who so chose could use a digital certificate issued by the state to digitally "sign" it.

No paper, no pen, no need to engage in negotiations about access. No heat, rain, cold, or table-carrying for petition circulators. No need to reduce the content of the initiative to a short slogan, since having it online along with explanatory and exhortory materials will mean prospective signers can examine the legislation's text and its supporters arguments at their leisure, 24/7.

And initiative sites can also include chat rooms for discussion of the initiative, FAQs (Frequently Asked Questions), links to related sites, audio and video clips discussing the measure, live webcasts (audio or video) of presentations on the initiative or debates between proponents and opponents, and so on, all of which would be difficult or impossible to bring to a mall and all of which would enhance the democratic process in general and the public understanding of every specific initiative in particular.

From the point of view of the election officials who need to sign off on the validity of the hundreds of thousands of signatures required to qualify a ballot measure, letting them be signed online with digital signatures ought to be seen as a dream come true. Currently, the paper-and-ink petitions submitted by initiative supports in one batch on the latest possible day allowed are not really checked very thoroughly. A small percentage of the signatures is checked, by hand, against the voter registration cards, and the results of this "random sample" are extrapolated to determine if enough valid signatures have been gathered.

But with digitally-signed petitions, the computers automatically, and almost instantaneously, authenticate and validate the digital signatures. This means that EVERY signature can be checked and authenticated, or rejected as inauthentic. The digital signing of initiative petitions is faster, cheaper, and every bit as private and sure as the current paper-and-ink method and allows for a more thorough validation process. Because it is all these things, Smart Initiatives would improve citizen access to the substantive content of initiatives and it would cut the cost of qualifying an initiative by several orders of magnitude.

Automating the signature gathering process will not mean that every proposed initiative would qualify for the ballot. The same number of citizens, now using digital certificates, would still need to sign the petition. But having the Smart Initiative system in place would mean that a good idea that found favor with 420,260 Californians who find their way to that measure's website would qualify for the ballot, without its supporters needing to raise a million dollars.

Still, this would only be the first step, since a majority of the voting public would still need to vote for the initiative when they encountered it on the ballot. But, at least in this first phase of the initiative process, putting it on the ballot, ideas and the will of the people could begin to count for more than cash.

It's been a continual source of frustration to me that the inside story of my efforts to legalize the use of the Internet for political and electoral purposes in California has gone largely unreported in both mainstream and technology media. I'm not saying my view is the only view. I am saying that more widely and deeply publicizing the issues, views, accounts, opinions, and preferences of all the players in this story would do a service for the people of California, help us get at the truth, and speed the day when we can move forward to use the powerful technology we've created for the important task of governing ourselves. This account, from my point of view, is an effort to get that dialog underway and out in the open.

A Brief History of the Struggle for Internet Voting in California

September 22, 2000

In 1996, I wrote the Virtual Voting Rights Initiative, which provided that:

107. (a) The Secretary of State shall design, develop, and implement a digital electoral system for the collection, storage, and processing of electronically generated and transmitted digital messages to permit any otherwise-eligible person to register to vote, sign any petition, and vote in any election, including applying for and casting an absentee ballot, using that system.

(1) The identify of the person submitting the digital message shall be established and the submission shall be authenticated as being the work product, political product, or actual and attributable communication of this identified person by the use of that person's digital signature, as defined in subdivision (d) of Section 16.5 of the Government Code.

(2) Each message may be originated in any electronic device, as long as the message is readable by an industry standard digital file server that shall be designated by the Secretary of State as the state electoral server and, in order to be valid and accepted for its intended purpose, shall be transmitted through a secure digital network that meets prevailing industry standards for these networks. Originating devices may include, but are not limited to, the following digital platforms: computers, touch-tone telephones, freestanding kiosks with touch screens, keyboards, or mice, personal digital assistants, interactive televisions, virtual personal assistants on phone networks, cable television systems, phone company or other fiber-optic networks, or utility company powerlines.

Petitions containing these provisions were circulated during the summer of 1996, but failed to collect the 400,000 plus signatures required to place it on the ballot.

In November, 1996, a state Assemblymember asked me for a copy of this initiative and, on December 2, 1996, offered it as AB44 to the state legislature. Not a thing happened until March, 1997, when the Secretary of State met with the Assemblymember, who, at the suggestion of the Secretary, amended AB44 to provide, not for the implementation of Internet voting in California, but for the creation of a Task Force to study its feasibility

This amended version of AB44 passed the legislature, but was vetoed by the Governor, in October, 1997.

For over a year, nothing happened, aside from the appearance of occasional newspaper articles in which I was quoted as saying that Internet voting would be a good idea and the Secretary of State was quoted as saying he was thinking about creating a task force to study the feasibility of Internet voting.

This piqued my curiosity, so I contacted his office and asked how he was able to create a task force to study Internet voting in light of the Governor's veto of legislation authorizing him to do so. Naïve political civilian that I was, I was told that the Secretary of State had had the authority to create such a task force whenever he felt like it, regardless of the fate of legislation specifically authorizing him to do so.

I then inquired further as to why, if that was the case, he had "suggested" that a pending bill mandating the implementation of Internet voting be "amended" to eliminate the proposed implementation and instead grant him the authority to do something he already had complete authority to do.

There was no answer.

After more than a year of hinting in the press that he'd appoint an Internet Voting Task Force, sometime in either 1998 or 1999, he did (the exact date is nowhere to be found on his website).

By December 27, 1999, I had received from the Office of the Attorney General of California the official Title and Summary to accompany my second try for Internet voting, the California Internet Voting Initiative. In the words of the Attorney General, the CIVI would have:

ELECTIONS. USE OF INTERNET FOR VOTER REGISTRATION AND VOTING. INITIATIVE STATUTE. Authorizes use of Internet for electronic voter registration and for casting ballots in direct primary elections, statewide general elections, special elections, and other public elections. Specifies standards for Internet voting systems. Requires Secretary of State to test and certify voting systems to accredit means of identifying and authenticating voters, to protect voter confidentiality, and to adopt rules and regulations governing Internet voting procedures. Requires counties to offer Internet option to all voters. Criminalizes efforts to interfere with Internet election system; specifies penalties. Preserves traditional voting methods.

On January 18, 2000, around the time I was about to start circulating this Title and Summary and the rest of the language that constituted the CIVI, the Secretary of State released his Internet Task Force Report, the conclusion of which was that there were so many security problems likely to happen that remote Internet voting must remain, at most, a distant prospect, and perhaps one never to be realized.

As far as I could tell, that's where things stood until today, when, because I'd heard that there were to be tests this November of non-remote Internet voting systems in

selected California counties under the auspices of the Secretary of State, I contacted his office.

Remote Internet Voting is Now Legal, at Least in California

Much to my surprise, I was told confidentially by a staffer in the Office of the Secretary of State of California that once the Secretary's task force on setting Internet voting standards completes its work (which could take a while because there are difficult issues to be resolved) and once certain definitional issues regarding "what is a ballot?" and related points are resolved by legislation, and once one or more companies provide systems for accreditation that meet the high standards set by the Secretary's specifications, then counties in California will be allowed to use these certified systems to carry out elections involving remote Internet voting, and, naturally, voters will then be able to use them to vote remotely over the Internet, from their laptops, desktops, or digital refrigerators, be they at home, the office, a desert island, or stuck in traffic (this latter site only if it hasn't been made illegal to use an electronic telecommunicating device while driving, unless they either pull over, or, in the case of traffic congestion, can plausibly and successfully make the argument in court that sitting in a traffic jam is not, legally speaking, "driving."

Thus, like T.S. Eliot's world, the battle for the right to vote remotely over the Internet in California ends, not in the bang of an election that passes an initiative legalizing it or by a vote in the legislature doing the same thing, but in the whimper of someone in the office of the state's highest election official letting it be known that it's been legal all along. We were just waiting for the man in charge to tell us it was. And now, however indirectly, he has.

So, just as the Secretary of State had and has the authority to set up Internet Voting Task Forces without explicit authorization by the legislature, he apparently also had and has the authority to certify systems for remote Internet voting without any explicit authorization by the legislature or the people of California acting through the initiative process.

So now we know that counties can begin offering remote Internet voting options to their voters just as soon as the Task Force on Internet Voting Standards finishes its work, software is presented that meets these standards, and the state legislature cleans up a few definitional odds and ends.

I'm glad to know that what I envisioned in the mid-90s, back in 20th Century, the right and ability of Californians to use the powerful tool of the Internet to work their political will through the electoral process is closer to being realized than ever and that, in principle at least, remote Internet voting is now essentially legal in California.

Of course, if all this is true, then it was also essentially legal in California four years ago. So why didn't the Secretary of State tell us then what's leaked out now? And how much more delay can we expect before we can actually exercise a right we've had

all along, only couldn't exercise, or couldn't demand faster progress in making it real, because the official responsible for safeguarding our voting rights chose not to trust us with that information?

What if they'd kept our right to free speech a secret from us, too? What if someday they do? If a political or civil right grows in the forest and no one can see it, how valuable can it be?

I knew in 1996 that Internet voting was feasible and desirable. It's more of both today. Let's demand it as our right and then use it to seriously improve how we govern ourselves. We deserve no less.

.

What if they some powerful government official someday tries to keep the existence of the Bill of Rights, or the U.S. Constitution, a secret from us, too? What if all the printed material mentioning our rights is replaced with WWF scorecards and McDonald's ads? What if AOL/TimeWarner/NewsCorp/Viacom/SBC/General Electric comes to own the Web, and deletes every mention there of our constitutional rights, replacing them, through the wonder of broadband, with repeats of Gilligan's Island and Burger King ads?

Or have they done that already and no one's noticed? If so, the least we can expect is for our elected officials to keep us posted about developments in their departments, OUR departments in a democracy, for example, that we can now legally vote over the Internet. Or am I being naïve, again?

One important aspect of Smart Initiatives is the creation and implementation of a process by which digital certificates will be provided to each citizen. This piece addresses some of the issues involved. It's not intended as a definitive solution, but a collection of suggestions for approaching the subject.

How the California Digital Signature Authority Will Arrange for the Issuance of Digital Certificates

September 22, 2000

From the Smart Initiatives Initiative, v. 1.0:

11790. (a) The Department of Motor Vehicles, the Secretary of State, the Department of Information Technology, and the county registrars of voters, shall collaborate to establish the Digital ID Issuing Authority of the State of California, whose mission shall be to efficiently and cost-effectively provide California residents with a high-level digital certificate in an easy-to-use form.

The Digital Signature Authority (DSA) (formerly the Digital ID Issuing Authority of the State of California), comprised of the Department of Motor Vehicles, the Secretary of State, the Department of Information Technology, and the county registrars of voters, shall set the standards for determining the adequacy of the digital certificates to be issued under this section and shall be responsible for their distribution.

In cooperation and consultation with private digital certificate companies and trade associations, the DSA shall develop these standards in such a way as to ensure that the certificates issued to Californians are of the highest possible quality, strength, and usability.

Once these standards have been established, they shall be promulgated by the DSA. Any and all digital certificate companies may apply to the DSA for certification as "Approved Digital Certificate Providers (ADCPs)". The DSA shall examine and consider the resources, capabilities, history and reputation of all applicant companies and shall certify as ADCPs only those which it determines are competent to issue digital certificates at the level of quality required under its standards and are capable of supporting them at the level of performance required under these standards.

The DSA shall send to each eligible Californian a letter officially notifying them of their eligibility to receive, at no cost to them, their own unique, private, high-level digital certificate. This notification shall be effected by USPS or other similarly-secure delivery service. What they receive will be, in effect, a voucher entitling them to one DSA-quality digital certificate, which they may, at their sole discretion, choose to obtain from any ADCP. They shall also be free not to obtain any digital certificate at all from anybody.

This letter of notification, which conveys to the citizen their digital certificate voucher, shall also contain within it one or more usernames, passwords, PINs, codewords, or other unique and confidential identifiers for the sole use of the citizen to whom the letter of notification is sent. These unique and confidential identifiers shall be used as part of the process by which the citizen redeems his or her voucher, unambiguously identifies him- or herself, and is entitled to receive their unique digital certificate.

The DSA shall include in this letter of notification a complete and up-to-date list of all digital certificate companies qualified as ADCPs, along with current contact information for each such ADCP, including their name, address, phone number, fax number, e-mail address and URL.

Each ADCP may undertake, at its sole discretion, any legal advertising or promotional campaigns, in any medium, it chooses to carry out in order to persuade Californians that they should redeem their state-issued digital certificate vouchers with them. They may make whatever legal arrangements they choose by which Californians can redeem with them their state-issued voucher for a DSA-quality digital certificate, provided that these arrangements are consistent with the methods set out by the DSA in their standards and specifications regarding the issuance of the certificate, especially as to security, privacy, confidentiality, and the establishment of the citizen/user's identity.

If a providing company wants to offer a rebate to a voucher-holder who redeems their voucher with them, they may, subject to state and federal laws against anti-competitive and monopolistic trade practices.

After selecting a vendor, Californians will then access the website of their chosen ADCP, complete a form by providing personal identifying information (including the PIN or other unique personal identifier provided to them in the letter of notification), choose a password that will allow them to remotely invoke their certificate, and be issued their digital certificate.

Depending on the preference of the user/citizen, these certificates may be stored on a remote server under the control of the DSA, or a remote server under the control of the ADCP issuing it, or on the hard drive, smart card, USB token, floppy disk, telephone, or other electronic device under the control of the citizen receiving the certificate, or on some combination of all these devices.

ADCPs shall be allowed access, in the most restrictive manner consistent with their being able to verify the submitted information, to databases under the control of the Secretary of State, Department of Motor Vehicles, or any other state agency, in order to thoroughly check and verify the identity of those submitting their vouchers in order to receive their digital certificates, provided that in every instance, the ADCP shall submit the information submitted to it by the citizen to the agency capable of verifying that information and that agency shall take that information, compare it with its own records, and inform the ADCP whether or not the data provided to it (the ADCP) is correct or not correct.

In no case shall the ADCP be allowed to ask for information from the agency and then use it to check the accuracy of the data it holds. In other words, the ADCP shall receive from state agencies information concerning applicants only in the form of confirmations or contradictions regarding the data it has received from citizen/users applying for their digital certificates and submitted to the agency, and shall never be given any more information than is strictly required to verify the accuracy of the information provided by

the citizen in order to establish their identity and their right to a digital certificate in their own rightful name.
Once the ADCP has determined that the applicant for a digital certificate issued by it is actually who they claim to be, it shall provide the citizen/user with the means of submitting a password of his or her choice to be used in invoking the digital certificate whenever they want to, whether the digital certificate is stored locally or remotely, or both. Incorporating this password into the digital certificate it is issuing, the ADCP shall generate a unique digital certificate for the user/citizen, and store it on its own server, the DSA's server, and/or send it by e-mail to the citizen/user, at the sole discretion of the citizen/user receiving it.

At the end of some time period (to be agreed upon between the ADCPs and the DSA and probably a period on the order of two weeks or one month), each ADCP shall submit an invoice to the DSA for payment for all of the digital certificates it has issued during the preceding period. DSA shall pay each ADCP according to the number of certificates it has issued under the guidelines established by the DSA, to citizens who redeem their digital certificate vouchers with that ADCP.

The amount to be paid by the DSA to the ADCPs for each voucher redeemed by the ADCP and submitted to DSA shall be determined though negotiations between the DSA and all of the ADCPs. Alternatively, The DSA may decide the amount it will offer an ADCP for providing a citizen/user with a digital certificate. Each ADCP may decide if it wishes to provide a digital certificate at that price. However, the DSA is responsible for assuring that every Californian receives a digital certificate in a timely manner. The ADCPs may not collude to extort the State of California to pay them an unreasonable amount for each digital certificate they provide. After a lot of haggling, what constitutes a "reasonable" payment for each digital certificate issued will probably be decided by the courts, after some delay and considerable expense.

All ADCPs shall be paid the same amount for providing digital certificates and associated services to those citizen/users redeeming their digital certificate vouchers with that ADCP.

All the ADCPs shall cooperate with each other and the DSA in order to establish and maintain the complete interoperability of certificates and authentication procedures provided by each and all of them.

The DSA shall hold the root certificate for all of the digital certificates issued under the provisions of this section. Each of the ADCPs shall be certificated by the DSA and its root certificate. The chain of trust for the entire PKI (public key infrastructure) here set out shall run back to the root certificate under the control of the DSA and, through it, to the State of California itself.

Under the authority of the DSA, the several ADCPs shall be responsible for maintaining the accuracy and up-to-dateness of their certificate lists, and shall, according to standards to be developed and promulgated by the DSA, establish and maintain Certificate

Revocation Lists (CRLs) that shall ensure the validity of all certificates on their active lists.

Renewals of these digital certificates shall be on the same basis as their initial issuance and distribution. When the time comes to renew the certificate, it is assumed that the default renewal will be with the citizen/user's current ADCP, but citizen/users may, at their sole discretion, transfer their registration/enrollment to another ADCP, which company shall receive their voucher and payment from the CSA for that renewal.

Citizen/users dissatisfied with the performance of their ADCP may ask that ADCP to transfer their enrollment to another ADCP, at no cost to the citizen/user. Each ADCP involved shall bear the cost of its part in the transfer. If everyone is willing to endure the tragic paperwork, an amount proportionate to the unused term of the certificate can be charged to the ADCP being transferred out of and a similar amount can be paid to the ADCP being transferred into. If possible, these transactions shall be conducted electronically and as soon as possible after the citizen/user asks to have his certificate revoked at the old ADCP and re-issued at the new one. Unless it is no longer functioning or accessible, the digital certificate being held at the citizen/user's original ADCP may be used to apply for a new digital certificate at the new ADCP, after which time the first certificate will be revoked and cancelled. If it is no longer available or valid or functioning or available, the poor citizen/user will need to apply to the DSA for a new PIN number and go through the application procedure again at the new ADCP. May we all be spared such a fate.

Digital certificates issued under the provisions of this arrangement shall be accepted for signing online petitions under the provisions of this section and may be used, at the mutual discretion of citizen/users and the relevant state agency, for the digital signing of forms, documents, or any transaction entered into together by the citizen/user and the state agency.

These digital certificates may not be used, however, in order to generate digital signatures in transactions between the citizen/user to whom it belongs and any non-governmental entity. However, these DSA-backed digital certificates may be used by any commercial or private entity as the basis for the issuance of a secondary digital certificate that may be used, at the mutual discretion of the user and the commercial or private entity, for the authentication of any electronic transaction between them.

I was glad to have David Broder report on my remarks at the Initiative and Referendum Institute's Conference in May of 1999. But I had some problems with the overall thrust of the book in which he included that report. Here's what I had to say:

Putting Democracy Back on Track:
A Reply to David S. Broder and "Democracy Derailed: Initiative Campaigns and The Power of Money"

October 9, 2000

David Broder is arguably the most important political columnist now working in the US. He has covered every presidential election since 1960. He's been writing for the prestigious Washington Post since 1966. I haven't. But I have been politically active since then, and I want to contrast some of his recent pronouncements with my own experience of real-world politics over the last 35 years.

Mr. Broder has just published "Democracy Derailed," in which he rails against the initiative process, saying that it has become corrupted from its Progressive and Populist roots and now serves as a means for rich dilettantes to meddle in a law-making process which rightfully, and constitutionally, belongs to the duly elected representative legislatures of the several states.

Now I'm the last person who wants to see our fundamental freedoms or even our current way of life violated and destroyed by the manipulations of power-hungry, self-financed autocrats paying to qualify initiatives and paying more to get them passed with slick ad campaigns. If that ever happened, it would be horrible. I'm ready to oppose such moves and I imagine there are enough others who feel the same way that this scenario will not occur (although, of course, it might).

The core of Mr. Broder's argument is that the initiative process violates the republican nature of our government, as established by the Constitution. (This even though many prominent initiatives passed in recent years in California have been thrown out, in varying degrees, by the courts.) The essence of the core of his position is that we are and must remain a representative, and not a direct, democracy.

Broder rightly points out that the Framers of the Constitution (especially James Madison), believed that the best form of government, the one most likely to protect fundamental liberties, and in their own words, "promote the general welfare," was one where governmental decisions were made, not by "the people" themselves, but by their elected representatives. Such an approach, Madison and Broder believe, works best because it filters the public's often-shifting desires through a system of checks and balances in which the actual decisions are made by selected representatives who are more capable of governing than are the masses of the population themselves.

Naturally, the direct legislation that is possible through the initiative process is anathema to those who, like Broder, believe that the best form of democracy is the

representative kind, not the direct. I would like to cite a few instances in my own experience that argue to the contrary.

Two years before Mr. Broder joined the staff of the Washington Post, in 1964, in May, I attended the Commencement ceremony at the University of California at Los Angeles, on a field trip from my high school, where I was a junior. Lyndon Johnson, recently ascended to the presidency, stood before thousands of us and said, "I will not send American boys to fight the battles that Asian boys should fight." Compared to Barry Goldwater's statements about almost anything, Johnson sounded like a good choice for someone who preferred neither to kill nor be killed in the then-obscure land of Vietnam.

I worked for Lyndon Johnson that year. I knocked on doors and told people to vote for Lyndon Johnson, because he was the Democrat and not the warmonger. He won. Shortly after winning, he began sending more and more American boys to fight in a war he'd told us should be fought by Asian boys. Almost fifty-eight thousand American boys, and girls, never came back from that war, except as corpses.

Lyndon Johnson had been elected to represent us. Of course, he'd lied about his intentions and he lied and he lied about Vietnam and what was happening there. So I showed up at the Century Plaza Hotel in Century City on June 23, 1967, a little more than three years after he'd lied to us at UCLA a few miles up the road, along with Dr. Benjamin Spock, Mohammed Ali (in the midst of appealing his conviction for refusing to fight in Vietnam), and hundreds of others to demonstrate our feelings of betrayal at how our representative in the White House was not representing us faithfully at all. The LAPD, claiming to represent "the people of California," responded to our peaceful efforts by beating more white people at one time than they ever had up to that time, a record that was probably eclipsed the following year, during the Democratic convention in Chicago.

Our representatives were giving representation a bad name.

As for the judicial branch, I once had a chance to ask Stanley Mosk, who could in fact be called the David Broder of liberal jurisprudence in California for his long, distinguished, record and the high repute in which he was held, a basic question about the law.

He was giving a talk at the Wilshire Temple in Los Angeles and told the audience that the legal conclusions enunciated by the California Supreme Court were not invented by the justices of that institution, but rather were found by them, pre-existing in something akin to the perfection of Platonic forms and then, like Moses on Sinai, brought down to the waiting multitudes. If that's the case, I asked him from the audience, as he towered over us down below, like Moses, or God himself, or like a Justice of the California Supreme Court (even though he was pretty short himself), if that's true, why aren't all decisions of the Supreme Court unanimous?

He wouldn't answer; he couldn't answer, he never answered, even when I tried to engage him in a friendly discussion of what seemed to me an interesting issue during the reception that followed his speech. He wanted us to think that judicial pronouncements were holy writ, that they were beyond time, or personality, or economic interest, when these elements are of their essence.

As for the Congress of the United States, the body that Broder's argument enshrines as the foremost repository of our freedoms and our well-being, let me only mention two brief phrases: "impeachment for high crimes and misdemeanors" and "campaign finance reform". With few exceptions (Bernie Sanders of Vermont comes to mind) no one can be elected to the House of Representatives, and certainly not to the United States Senate, without spending hundreds of thousands of dollars that come, almost by definition, and certainly in fact, either from wealthy individuals or big corporations.

Minor differences with current policy are tolerated. But no one is elected to "represent" us who is not either in fundamental agreement with the priorities of those doling out the money or able to act as though he or she is in fundamental agreement with these priorities. This is representative democracy, but it is not democracy in which the people are represented. It is representative democracy in the sense that special interests of various types are represented, and are represented to the extent that they can afford to be.

In fact, once you realize the congruity, or the identity, of today's special interests with what Madison called "factions," you can begin to realize the terrible irony inherent in the fact that our constitutional system, designed to protect against power grabs by instituting a system of checks and balances and representation, has, though that very system, led to a situation where "faction" has overcome the barriers raised against it and has enshrined itself under the name of its opposite, which is democracy.

So, while Mr. Broder may make a superficial, or theoretical, argument showing that representative democracy is good and direct democracy is bad, the facts of my own experience, and I suspect the experience of not a few others, do not convince me that so-called representative democracy, with checks and balances, an independent judiciary, a popularly-elected Congress, and an indirectly-elected President (through the Electoral College) is, to coin a phrase, all that great.

Suffice it to say that every president since the 60s has disappointed in one way or another. Johnson and Nixon sent tens of thousands of Americans and millions of Vietnamese and Cambodians to their deaths without a constitutionally-required declaration of war. Reagan waged an illegal war in Central America and presided over the creation, by his former campaign manager, William Casey, of an "off-the-shelf" extra-constitutional shadow government.

Congress responds to the needs of its stockholders (I mean its campaign contributors) far more than it does to its customers (I mean us citizens.)

The U.S. Supreme Court rules that the Food and Drug Administration cannot regulate nicotine (to which millions are addicted and if not as a drug, then as what, a harmonica?), but allows thousands upon thousands of people to be incarcerated for possessing small amounts of marijuana. Who's being represented by that decision?

To summarize, it seems evident that representative democracy in America, which Broder lauds as the highest form of self-government, has, over the last 35 years, been so rife with corruption, venality, hypocrisy, self-promotion, and banality as to render his argument seriously invalid.

But don't rely on my limited experiences and my possibly idiosyncratic take on politics since the mid-60s. Consider the words of architect Christopher Wren, who famously left his own epitaph within one of his designs, St. Paul's Cathedral in London. He wrote (here translated loosely from the Latin), "If you're looking for a monument to me, just look around."

The disdain, apathy, even vilification that most Americans now direct towards their political institutions and especially the politicians who populate these institutions, is plenty of monument to the functioning of representative democracy in the U.S. since 1965. With or without relying on the evidence and reasoning I've submitted here, most Americans have, intuitively or logically or both, come to hold an extremely low opinion of the institutions of "representative self-government" that now exist.

Only half the registered voters voted in the national elections of 1998. That's half of registered voters, not eligible voters. A new city charter was adopted Los Angeles in 1999 by fewer than 10% of the registered voters in the city. Who's being represented here?

With legislators who've been captured by those with the biggest checkbooks, with Presidents who abandon the platforms they run on in order to satisfy the needs or whims of their public or private patrons, with courts marching to a combination of their own idiosyncratic and often ideological drums, where is the representation of the people in this "representative democracy"?

It's possible that some kind of out-of-control initiativocracy could strip away the Bill of Rights and enslave us all. It's possible we've reached the end of history and the end of politics. But I think it's more likely that, despite how loosely the spirit and often the letter of the Constitution have been construed by all branches of the government in recent years, as the idyllic economic and social milieu we've recently been enjoying gives way to rising oil prices, increasing unemployment, a precipitously declining stock market, falling consumer confidence, and a rising chorus of demands for a foreign war to keep oil prices low and the SUVs rolling, we will, unless anarchy (in the bad sense) ensues first, once again turn to politics and the government to resolve the decisions these changes will require.

It will matter then, even more than it does now, that we be able to enact into law and then execute as law, the decisions we make collectively as a people. Representative democracy has been the structure for making the public decisions that we've used during the last 35 years, and beyond that, back to the founding of what we call, of course, the Republic.

David Broder believes that this form of democracy, representative democracy, is its only true form. And he knows an awful lot about both the theory and practice of our politics, which is called "democracy." But he's not the only one who's experienced the politics of "representative" democracy in recent years. Some of the rest of us have too. And some of us don't feel all that represented.

Maybe something a little more direct, even with the new problems that it may bring, maybe new forms of direct democracy no one's thought of yet, maybe something built around the Internet and not the horse-drawn carriages that brought James Madison, Benjamin Franklin and the others to the Constitutional Convention in Philadelphia 211 years ago, might do for us what the original Constitution did for them then: put the best ideas in the world to work for the people of this country and, by our example, everyone else in the world.

In a world where banks, stock markets, and entertainment conglomerates send money, equities, and programming around the globe at light speed and where citizens play at decision-making by punching holes in computer cards, whose interests are likely to prevail, those of citizens, or the welfare of global capital? This essay suggests an answer to this problem.

Global Electronic Democracy the Answer to Global Corporatism

October 10, 2000

Despite the fact that many of them find governments as repressive and reprehensible as they find multinational corporations, the "anti-globalization" forces recently in evidence in Seattle and Washington, D.C., still sometimes suggest that governments can help them in their efforts to counter the pernicious effects of global capitalism, generally by implementing laws to limit the power of corporations to do one thing or another.

But they do not, in my view, go far enough. Against the overwhelming and growing power of high-technologized global capital and transnational corporations, what entity can possibly countervail but a vigorous, democratic, decentralized, powerful and equally high-technology global government?

Feared by many as a sword that would destroy individual freedom, such a democratic and electronic institution may now be the only shield capable of protecting the individual and collective interests and rights of 6 billion people against the increasingly seamless control now wielded over the economy of the planet and the minds of its inhabitants by the interlocking corporations that provide us all with food, transportation, entertainment, and visions of what life is about (consume entertainment, consume "fun", consume sex, consume, consume, consume).

Obviously, a Big Brother-like government that surveils, arrests without cause, tortures, disappears, and murders its citizens is a completely bad thing. But it hasn't required the existence of a world government for the emergence of this kind of behavior by separate national governments. Nazi Germany, Cambodia under the Khmer Rouge, Argentina's dirty war, and plenty of other genocidal regimes have reached this depth of depravity while remaining merely national jurisdictions.

Nor is the kind of non-world government that characterizes the present United Nations what I have in mind. This is truly a government-to-government operation, featuring an illustrious aggregation of world-class representatives and bureaucrats who can sometimes do useful humanitarian work but which has mostly been, since its founding in the aftermath of the Second World War, a reflection of the alliances and strains in world politics, not a means for resolving them nor an instrument to challenge existing power relations, either between states or between economic institutions and the people or nations they effect.

Recent visits to the government websites of various countries revealed to me that politics is politics and elections are elections, wherever you go. The website of Brazil led me to an electronic voting booth for candidates in one of its states. The website of a now-united Germany impressed me with its Flash graphics and thorough coverage. Just as they are increasingly listening to the same music (or variations thereof), following the same news stories, and worrying about the same issues, in their local and global manifestations, world citizens are also having more or less the same electoral and political experiences.

Candidates are more or less honest and campaigns are more or less fair. Some issues involve matters that can convincingly be characterized as local. Others, like those involving world trade, investment, global pollution, and such, are clearly transnational in scope. As things now stand, citizens in specific localities elect governments that then negotiate with each other over those issues that effect them all. These government act as (classic) intermediaries, representing the desires of their (often conflicted) constituencies, taking into account the importuning of their campaign contributors, their desire to please the media, their own career considerations. Sometimes the results are advantageous for the majority of those effected, but not always.

These problems are endemic, and have characterized political life everywhere since the beginning of time. There has now arisen, however, a technology that is famously capable of disintermediating transactions, and does so already, on a global scale. It is the technology that now dares to speak its name as a solution for previously-intractable political problems: the Internet.

As we are already starting to see, the Internet has the ability to directly connect buyers, sellers, advertisers, customers, and even elected officials and constituents. As Internet technology continues to evolve and adds more and more capability to connect people and institutions in increasingly sophisticated and subtle ways, there is a corresponding increase in its ability to provide the infrastructure for a global government that is more, not less, supportive of individual freedom and human rights, while at the same time allowing everyone effected by a governmental decision to participate directly in the making of it.

It's not my intention to set out in any detail the form that such an electronic global government ought to take. I want merely to point out that only a powerful global government will have the ability to fend off the power grab of the international corporate armada, as well as to deal with issues of global scope such as resource depletion, population growth, environmental contamination and collapse. I also want to make the point that an Internet-based, democratic and participatory form of government can create systems of governance for all of us worldwide that are at least as supportive of human rights, personal dignity, and justice for all as the best of today's governments and could represent a significant improvement for many nations in comparison with their current system of governance.

An integrated, transnational, electronic democracy would allow for a worldwide concurrent evolution of our governments, economy, cultures, and lives in a way that would build upon and go significantly beyond the already-strong decline of the nation-state as the primary organizing tool for government and, in many cases, personal identity. The global economic system has long since evolved past its national stage. The multinational or transnational corporation is actually a "post-national" corporation. It draws on world capital for investment, executives, workers, and markets. Its managers and owners are loyal to their class and their corporations, and to the concept of a single world as the playing field for their economic exploits.

Meanwhile, national leaders, even the most talented and compassionate, and all those they lead, cannot successfully compete with institutions with limitless resources and limited responsibilities. Former California Senator Alan Cranston, such a strong defender of freedom that he became the only American citizen ever sued by Hitler (for intellectual property violations involving the American publication of Mein Kampf, if you can believe that), and many others associated with him worked for years on behalf of the concept of World Federalism. Under this model, nation states would unite like the thirteen original colonies did to form the United States. It was a shocking idea in its time, and, as you can see by looking around at the world, one which has never been realized.

Now we need something more, something deeper. To confront the powerful thesis of global capitalism organized through the post-national corporation and its attendant institutions, we need the antithesis of global government. We need a global government that is democratic, protective of individual and group rights, electronic, participatory and open. Only people who are using all the powerful technological and organizational tools that have raised the modern corporation to world ascendancy have any chance of controlling its power or turning that power, tempered and informed by their own desires, to their own, more humane, purposes. We must do that now, and move towards the creation, under the umbrella of that global government, of a global civilization that we can be proud of and which will nurture us, individually and collectively. We need to create a humane social infrastructure such as this, one which can and will endure and evolve as we move into the future, or forego that opportunity, and enter an extended era of brightly-lit slavery.

By combining a number of applications of the Internet to the political and elections process, it would be possible to combine the benefits of direct participation by citizens and the important intermediating contributions that can be made by elected representatives. This essay addresses these applications and suggests a possible synergy between the citizens and their government, mediated by the Net.

Real Time Democracy

October 10, 2000

Thirty-five thousand, seven hundred, and sixty-five Arizona Democrats have proven that Internet voting is viable, cost-effective, secure, and a great way to bring the previously-uninvolved into the electoral process. Now that these facts have been established, the obvious next step is to bring Internet voting to all American citizens. This can be done through legislation, administrative decisions, or the initiative process.

But while we are doing that, we shouldn't forget three other ways in which the Internet can be put to work in the service of democracy. All of these steps, taken together, will move us closer to "real time democracy." They are:

1. the electronic signing of online petitions to qualify initiatives and referendums for the ballot, with a constantly-updated online display of the current number of valid signatures collected

2. the instantaneous inspection, certification and reporting of campaign contributions

3. the provision of systems allowing elected officials to constantly take the pulse of their constituents' legislative and policy issue preferences

The core Internet technology that makes Internet voting possible also makes it feasible to deploy and deliver these additional democratic services, the existence of which will facilitate and make transparent the inner workings and state-of-play of various parts of the democratic process.

Once the political parties and the state identification agencies (usually the Department of Motor Vehicles) can find the will and the time to sit down with the digital ID people who make Internet voting work, and possibly with the smart card manufacturers, it will be relatively straightforward to provide each citizen with a digital ID comparable to their driver's license, or as part of their driver's license.

This digital ID will, in conjunction with an installed Internet voting system, allow citizens to vote online, and also allow them to digitally and definitively sign online documents, including initiative petitions.

Using this same digital ID, all campaign contributors would be able, if required, to submit a description of their proposed contributions to the state or federal authority

responsible for enforcing campaign finance laws. If the proposed contribution is legal, it will be certified as such by the controlling agency, the funds involved will be electronically transferred from the contributor's account to the recipient's, and the facts of the contribution will be instantaneously posted on the agency's website, where everyone who wants to can see them.

Once the citizenry is equipped for electronic participation in elections, petition signing, and campaign contributing, it will have everything it needs by way of tools and training to allow elected representatives to set up websites that allow all their constituents, and only their constituents, to constantly keep their legislators informed as to how they feel about upcoming floor votes, possible trade-offs in legislative negotiations, and long-range priorities and concerns.

Using the technology already proven to work in Internet voting, it would be easy to construct a system that would let constituents cast advisory ballots on all manner of issues facing their representatives in the state capital. This system, like the Internet election systems themselves, would allow each citizen to cast a secure and, if they choose, an anonymous, ballot dealing with issues of interest to them and/or chosen by the official. The main difference between this procedure and a regular election would be that the electorate could cast their ballots on a daily or weekly basis., not a biennial one.

The results of these secure constituent polls could be made public, on a real-time basis, as each vote is cast. Elected representatives would be free to follow their constituents' expressed preferences, to take them into account, or to ignore them. The voters, of course, would be equally free to consider the responsiveness of their representatives to their digitally-articulated preferences in deciding, the next time they vote over the Internet, whom they wanted to represent them in the legislature.

This piece puts Smart Initiatives in the context of the voting meltdown in Florida. A shorter version of this article was published as an op-ed piece in the Sacramento Bee on November 26, 2000. You can read it there at:

http://www.sacbee.com/voices/news/voices05_20001126.html

After Florida, What?

November 12, 2000

Many people are saying that the voting mess in Florida demonstrates the need for Internet voting now. The situation in Florida is the combined result of using antiquated technology within an outmoded administrative model in a political context that failed to generate the clear margin of victory needed to obscure the overall dilapidation of the entire system.

But converting a system based on IBM 360 technology from the mid-60s to a remote Internet voting system, and expecting voters who were baffled by stylus-and-punch-card technology to instantly grasp drag-and-click systems, may be overly optimistic.

I voted this time on a touch-screen system from Global Election Systems, here in Los Angeles. It was fast, fun, and, I assume, accurate. I was validated to the system with a smart card that was personally programmed for me by an election worker, who "charged" it with the right to vote once in my districts after I signed and gave her the back cover of my voter pamphlet, which had been mailed to me.

This was at least as secure as the standard procedure here, which prohibits election workers from asking for ANY ID from prospective voters. If I, and all other voters, had already had a smart card that contained my name and address, we all could use that card to vote on these touch-screen machines, without any additional intervention from on-the-scene election workers, who could then concern themselves principally with helping people figure out how to insert the cards in the machine and how to select by touch the candidates and initiative and referendum options of their choice.

But this approach is not remote Internet voting. And I believe that at this point in time, it is a better way to ascertain the will of the people

Remote Internet voting has yet to overcome some important technical and administrative problems. The most interesting one, in my view, is what I call the problem of "anonymous authentication." Electronic voting, under our democratic system, needs to be anonymous. That is, the authorities need to be unable to determine WHO has cast any particular ballot. On the other hand, each voter needs to be authenticated, one way or another, to a greater or lesser degree of certainty.

With paper ballots of any kind, the authentication happens when the election worker checks the voter in and thereby checks his or her name off the list of people who are entitled to vote again. Remote Internet voting systems can do this by identifying a person wanting to vote by means of a PIN, a password, or, more rigorously, a digital certificate.

Paper ballots are anonymized by tossing them into the ballot box, where the uniformity of every ballot (apart from their content) effectively makes it impossible to know which person cast which ballot. Thus are voters able to be both anonymous AND authenticated, using paper ballots.

While it may be theoretically doable, no one has yet explained to me intelligibly and persuasively exactly how it's possible to simultaneously authenticate and anonymize a ballot in cyberspace, where there is no way to create the virtual equivalent of a ballot box in which to effectively shuffle the electronic ballots so no one can tell who voted how. Any system that attempts to anonymize the ballot of a person already authenticated to vote is going to leave an electronic trail of the process by which it has attempted to perform the anonymization. Working backward along that trail will eventually reveal whose ballot it was that was "anonymized," which is, of course, no anonymity at all.

One can argue that by making it illegal to "de-anonymize" electronic ballots, the practice can be prohibited. When has making something illegal ever succeeded in keeping it from happening?

There are other technical problems with Internet voting. The California Task Force on Internet Voting has highlighted most of them, including the use of viruses and Trojan horse programs to block, change, or modify remotely-voted electronic ballots, and the use of denial-of-service attacks to effectively shut down election servers during the crucial and limited hours of an election.

There is also the infamous "digital divide," much discussed already, which is regularly invoked, not as an argument for providing every citizen with the means and the training to effectively use the Internet for civic activities, such as voting, but as a reason for denying everyone the opportunity to so use it.

Here is a final note on the lessons of Florida as they apply to remote Internet voting. If and when these technical and social obstacles to the use of the Internet for remote voting are overcome, we should decide now that the software used for such a system be Open Source. Open Source software means software where the computer code that runs a program is in the public domain. It is freely available on the Net. It can be examined and inspected by anyone who wants to.

Making Internet voting software Open Source will eliminate the undesirable situation where counties use propriety Internet voting software programs that are closed to the public, which makes the public jurisdictions using them dependent on private, for-

profit companies for the maintenance and possible upgrade of the code that they, and their citizens, depend on to give them free and fair elections.

Not using Open Source remote Internet voting software will further undermine public confidence in the election system, even before it is used at all. As we know very clearly from the current imbroglio in Florida, it is confidence in the system that is most damaged by fouled-up election procedures, and without which the continued viability of that system comes into question.

This is without mentioning the cost savings available to voting jurisdictions who get their Internet voting software under a licensing agreement that charges them nothing at all for the code, while allowing private companies to make money on Internet voting by providing documentation, training, and support to the counties. In the wake of the Florida debacle, we might even hope that all the states (whose responsibility it is to conduct elections) will decide to spend substantial sums to upgrade voting operations. As counties everywhere undertake to upgrade their voting operations, the situation will be ripe for local voting authorities to take advantage of an Open Source approach that gives them the code for free and allows them to contract for support services that will allow them to re-invent themselves at a much high level of competency.

Open Source voting code will also allow the collective expertise of the computing and the political communities to be used to debug and upgrade the quality of any particular Open Source voting software, including both interface and security aspects.

Given all this, along with the clear message from Palm Beach County that the old ways are not good enough, how can we put the power of the Internet to use NOW in a way that is fair, useful, and establishes the basis for its further development as a tool of democratic self-governance?

Not every state has the initiative process, but almost half of them do. The initiative process (and the associated processes of referendum and recall) was instituted at the urging of the Progressive movement around the turn of the 20th century. Hiram Johnson, the Progressive Party governor of California at the time, successfully championed its adoption in that state in 1911. It was designed to allow the people of California to circumvent the state legislature, which was then famously a captive of the era's special interests, especially the railroads, who were maintaining a stranglehold on farmers who wanted to ship their produce to the East.

Today, however, the initiative process has in many ways become an equally famous captive of this era's special interests. The principal means of this control resides in the fact that it now takes about one million dollars to qualify an initiative measure for the ballot in California. This cost, in turn, is the result of the fact that antiquated and inefficient methods are still being used to collect and process the nearly half-million signatures required to put a statutory initiative on the ballot, or the nearly 800,000 needed to put a constitutional amendment there.

It is in the initiative process that the power, speed and efficiency of the Internet can be used to give the people more say in how they govern themselves, without running up against the problems apparently inherent in remote Internet voting.

By allowing citizens to sign initiative petitions over the Internet, the laborious check-by-hand validation process that costs the taxpayers so much and makes the initiative qualification process take so long, and be so uncertain, could be replaced by the fast, cost-effective, and elegant use of digital certificates to authenticate the signatures.

Some of this uncertainty, by the way, comes from the use of random samples and arcane formulas for projecting signature totals that are routinely used in qualifying every California initiative. If you enjoy "hanging chads" as the critical determining factor in electing the President of the U.S., you ought to also enjoy the mysterious ways in which initiative petitions are now processed to determine their eligibility for consideration by the voters of California.

Public Key Infrastructure (PKI) and its associated elements, including Certificate Authorities (CAs), Repositories, Revocation Lists, Public and Private Keys, Digital Certificates, and Digital Signatures, have been created precisely to allow people to do business in cyberspace, to definitely and legally participate in all manner of commercial transactions over the Internet. The banking, insurance, and HMO industries worked long and hard to see to it that the recently-passed and promulgated E-Sign Bill reflected their interests in the transition to e-commerce. Consumer groups were also heard from before this landmark bill became law, insuring that consumers would be protected from any negative effects of allowing digital signatures to be used to enter into contracts online.

Now that the private sector and the consumer movement (not to mention the House of Representatives, the Senate, and the President) have all agreed on language legalizing digital signatures for transactions on the Web, it's time to apply this new law (it went into effect on October 1, 2000) to transactions between citizens and their government.

While the E-Sign Bill legalized digital signatures as an instrument for projecting one's legal identity into cyberspace, it did nothing to provide individual consumers or citizens with the digital certificates they will need to take advantage of this law in the commercial, political, or e-government spaces.

Enter the Smart Initiatives Project, a group working to fill the digital certificate gap and, simultaneously, further legalize the use of digital signatures created by digital certificates for the specific purpose of signing initiative and other official petitions online.

The Smart Initiatives Project drafted the Smart Initiatives Initiative and shepherded it through the first steps of the process required to qualify an initiative in California. Now, using the Net as intensely as possible for media and public education, recruitment and coordination of volunteers, fundraising, and even for the distribution of actual petitions, the Smart Initiatives Project is attempting to work within the antiquated

system that is blocking access to the powerful initiative tool for ordinary people and organizations in order to replace that system with one that takes advantage of the Internet's reach, speed, and ubiquity so as to open up the initiative process to new ideas and new participants.

Not only are Smart Initiatives a good way to re-furbish the initiative process in states that already have the initiative process, but it is also a great form in which to introduce the concept of initiatives into states that don't yet have it. And while I don't myself at this time support such a reform, those who feel that the states are unimportant enough and national majorities significant enough to justify abolishing the Electoral College (this was Senator-elect Hillary Clinton's first post-election recommendation) might consider adopting a National Smart Initiative System (NSIS) as the proper form for a national initiative process.

But what about the objections listed above to Internet voting? Don't they also stand in the way of moving the initiative process into cyberspace? Actually, they don't.

"Anonymous Authentication" is definitely NOT a problem for the Internet-based signing of initiative and other official petitions. The essence of signing any kind of petition, including an official one, is that by doing so, the signer is publicly declaring him or herself in favor of whatever it is that the petition is calling for. There is no need, therefore, to keep the names of the signers anonymous. Even the idea of anonymously signing a petition is kind of nonsensical.

There are, moreover, already in place certain safeguards to protect the privacy, if not the anonymity, of citizens who sign official petitions. All the laws that currently protect the privacy of petition signers are carried forward under the provisions of the Smart Initiatives Initiative. In fact, since signers' names will not be visible on paper forms when people sign petitions online with digital certificates, the signers will probably enjoy more privacy using electronic methods than they now enjoy using pen-and-ink methods.

The denial-of-service attacks that shut down a number of Net powerhouses earlier this year, and which could just as easily shut down an Internet voting site, would be irrelevant in the context of Smart Initiatives. Since under current law initiative petition signatures are collected over a 150-day period, and not just a single day, a concentrated attack designed to shut down a particular server hosting one or more circulating initiative petitions would be of marginal significance. Nor is there anything in the provisions of the Smart Initiatives Initiative that would prevent initiative proponents from hosting their initiative petition on multiple servers, creating redundancies that are of the essence in the Internet's architecture and which would render much more difficult the efforts of lawbreakers to violate the integrity of the online signing process.

As for viruses and Trojan horse programs that would take over citizens' computers and use them to sign petitions illegally, common sense tells us that any cracker capable of overriding or subverting a computer owner's control of his or her machine and

using their digital certificate for mischievous and/or nefarious purposes is more likely to want to use that stolen control to transfer funds available online to their own account than to manipulate code to unlawfully sign an initiative petition.

Furthermore, by adding a confirmation procedure to the signing process, it would be possible to ask every digital signer of a petition to verify that they have indeed chosen to sign a particular petition.

As to the "digital divide," under the terms of the Smart Initiatives Initiative, every adult Californian with either a driver's license, a state ID card, or a voter registration card will be entitled to a smart card containing their digital certificate, at no extra cost to them. This means that citizens without computers of their own will be able to use their smart cards to authenticate themselves over the Internet, using any current or future devices that provide for such access.

At the present time, this would include computers at Kinko's, in schools, libraries, or in public kiosks. In the future, as broadband and wireless ubiquity provides easier access from more types and more instances of Internet devices, these cards (and their successors) will allow just about everyone to avail themselves of the right to sign initiative petitions online granted them by the Smart Initiatives Initiative.

These are, I think, persuasive answers to questions that can be raised against the use of the Internet to sign initiative petitions. There are, in addition, many positive reasons to support this project. I've listed ten of them below, and added some links to related sites.

You can learn more about the Smart Initiatives Initiative by visiting its official website at:

http://www.smartinitiatives.org

Top Ten Benefits of the Smart Initiatives Initiative, which will:

1. Save the state and counties time and money in the processing of initiative petitions

2. Provide for the definitive authentication of EVERY petition signature, not just a random sample

3. Counter the efforts of opponents of the initiative process who want to raise signature requirements or shorten collection periods, or do both, or exclude certain people from collecting them, or prohibit the paying of signature gatherers

4. Reduce confrontation between signature gatherers and private property owners who don't want their property, such as malls, shopping centers, and post offices, used for collecting signatures on initiative petitions

5. Make it easier for citizens to sign initiative petitions and to know and understand what they are signing

6. Reduce the cost of qualifying an initiative by a factor of up to one hundred times, from a million dollars to the ten thousand dollars needed to build a first-class website, thereby allowing individuals and groups without million dollar budgets to participate in the initiative process

7. Build the infrastructure needed to provide citizens with a wider range of e-government services at all administrative levels, thereby increasing citizen convenience and reducing government (and therefore taxpayer) costs for many government services

8. Provide citizens with the means to participate more easily and more often in a wide range of existing and emerging e-commerce transactions, including signing contracts online under the provisions of the recently-passed federal E-Sign Bill, all of which will stimulate productivity growth and general economic growth without inflation, and which could result in lower taxes

9. Position states that adopt it on the leading edge of e-government and e-commerce, thereby competitively advantaging their citizens and businesses as they move into the 21st century

10. Protect the environment by allowing for more political and economic activity with less travel, energy consumption, and resulting ecological degradation.

A briefing paper published in 1999 by the Progressive Policy Institute entitled: "Jump-Starting the Digital Economy (with Department of Motor Vehicles-Issued Digital Certificates)" explains the background of the Smart Initiatives Initiative and can be found at:

http://www.ppionline.org/ppi_ci.cfm?contentid=1369&knlgAreaID=107&subsecid=126

To hear an audio and video discussion of the virtues of Smart Initiatives click here:

http://www.eyada.com/redirect/redirect_bof.cfm?id=6&date=101600

There are more text and audio links on the Media Wall at the Smart Initiatives website at:

http://www.smartinitiatives.org/English/mediawall.html

To join the Smart Initiatives Mailing list, click here:

http://www.smartinitiatives.org/English/mailinglist.html

To make a contribution to the Smart Initiatives Project, click here:

http://www.smartinitiatives.org/English/donationsset.html

To download a copy of the Smart Initiatives Initiative for signing and mailing in, click here:

http://www.smartinitiatives.org/English/petition/petition.html

Here are the titles and links to some articles about Smart Initiatives and related subjects:

1. Internet Voting Circa 2002 http://ic.voxcap.com/issues/issue228/item4339.asp
2. Could the Internet Change Everything? http://ic.voxcap.com/issues/issue249/item5418.asp
3. Putting the "E-" in E-democracy http://ic.voxcap.com/issues/issue294/item6421.asp

Links to all three papers can also be found at: http://ic.voxcap.com/bios/bio956.html

My early, unsuccessful, efforts to raise money in support of Smart Initiatives got me thinking and led to the following observations.

Some Notes on the Political Economy of Qualifying an Initiative

November 14, 2000

When I started the Smart Initiatives Project, I imagined that most of the million dollars I'd need to pay a professional signature gatherer to collect the nearly half-million signatures required to put an initiative measure on the ballot in California would come from the rich people who were already putting initiatives of their creation on the ballot.

I couldn't have been more wrong.

I might have seen it coming. Back in the spring of 1999, when I was a panelist and speaker at the Initiative and Referendum Institute's conference in Washington, D.C., I encountered Ron Unz, Silicon Valley entrepreneur and the person who'd used a lot of his own money to kill bi-lingual education in California through the initiative process. I asked him if he'd be interested in helping me put the California Internet Voting Initiative on the ballot. He brusquely rejected my question, indicating a total lack of interest in doing anything of the kind.

Months later, when David Broder's reportage on this conference appeared, in his book attacking the initiative process, "Democracy Derailed: Initiative Campaigns and the Power of Money," I became privy to the feelings, if not the logic, behind Mr. Unz's reaction.

> From page 237 of David S. Broder's "Democracy Derailed: Initiative Campaigns and the Power of Money":
>
> He was followed by Marc Strassman, the founder and leader of the Campaign for Electronic Democracy, an Internet-based national effort to persuade states to allow electronic voting and—where the initiative process is available—the collection of ballot-measure signatures via the Internet. If the legislatures see the beauty, simplicity, and economy of this scheme, and Congress does the same for the nation, "we can have initiatives, voting, politics, and government at the speed of thought," he said. "What about the people who don't have computers?" a member of the audience asked. "They will get cheaper and smaller," Strassman replied, "and a liberal government would want to give computers away" to those who need them. Some might be skeptical, but Rick Arnold [owner of a signature-gathering company] assured the audience, "Democracy will

be changed by this technology." He added with a smile, "I'm looking for another job myself."

Somewhat surprisingly, given his own use of the initiative, Ron Unz said he was skeptical of this vision. "We'd have eighteen hundred initiatives on the ballot in every election in California," he said, "and people would get sick of it, just like they're sick of government-by-polling today. We should raise the barrier, discourage people from putting up initiatives. There should be some kind of merit test." But the proponents were not fazed. "The legitimacy of an idea would be measured by how much support it has," Strassman said.

Published by Harcourt, Inc.

Indeed, why should multi-millionaire Ron Unz, who can place an initiative on the ballot anytime HE wants to, want to see a change in the rules that would let people and organizations WITHOUT a million dollars qualify an initiative for the same ballot?

Why should multi-billionaire Paul Allen, who can and did place an initiative on the ballot in Washington State to provide public funding for a stadium for a sports franchise he owned, AND WHO EVEN PAYED FOR THE ELECTION, want to let others, who weren't co-founders of Microsoft, get in on the fun?

Right now, I'm attempting to get funding for the Smart Initiatives Initiative from an organization which is rightly famous for funding a whole series of state initiatives for the purpose of implementing their particular take on the reform of a pressing public issue. They have sometimes encountered opposition, even vehement opposition, from grassroots organizations who also care about the same issue that is the focus of this national organization's concern.

Given the vast disproportion in monetary resources between the grassroots volunteer groups and the extremely well-funded national organization, it is almost always the national organization that takes and maintains control of the initiative campaign in any particular state. This means that the big group decides on the content of the initiative and on the way the campaign to qualify and pass it will be run.

As a result, grassroots organizations often feel excluded and resentful.

Recently, while I was discussing the inclusion in the national Smart Initiatives campaign of a local organizer who was seen by the director of the national organization as a disruptive nuisance, both the national director and I simultaneously realized the dynamic that would be generated by the qualification and implementation of a Smart Initiatives Initiative in a state where local groups wanted to proceed in one direction

while a large, well-funded national group focused on the same issue wanted to proceed in another.

While the big group could qualify their version of an initiative by spending money, the small, local group could qualify theirs by posting it on the Net and attracting signatories to their site, which might, for example, be called SignSite.org. This would remove the competitive advantage that the large group had by virtue of its money and would put the two proposals, and organizations, on a virtually equal playing field, at least as far as qualifying their initiatives.

Of course, the deep-pocketed national organization could always outspend the smaller group in paid advertising in various media, including even the Net. But maybe the national group wouldn't want to get into a public fight with supporters whose position on the issue being addressed only varied from theirs in certain, perhaps not too important particulars. In that case, they would need to negotiate from a more equal position with people and groups they could, before the advent of Smart Initiatives, more or less completely disregard.

The result of these negotiations would certainly be more favorable to the local groups than it would have otherwise been, absent Smart Initiatives, which would let them qualify their initiative at a fraction of what it normally costs to do so with paid signature gatherers.

Does it make any sense at all, then, for the big, well-funded national organizations who seek to implement their policies of choice on a national basis to fund an initiative, the Smart Initiatives Initiative, that would strip them of the advantages they now enjoy and reduce them to campaigning on the merits of their position against others who feel just as strongly as they do but who lack their vast resources?

To ask the question is to answer it.

And this is only that part of the story involving "progressive," "reformist," and "liberal" groups. Nothing really needs to be said about how this dynamic applies in the case of huge corporations without even an avowed commitment to the public good, but only an intense desire to maximize profit for shareholders through the bending of public policy to their own parochial and selfish interests.

What all this means is that if Smart Initiatives is to succeed, it must succeed on the strength of volunteer efforts and relatively small contributions donated by individuals and groups who know that the initiative process is a powerful tool for reform and that it can be made even more powerful once the requirement of infusing massive amounts of cash into the process before one can be admitted to it is removed.

Perhaps David Broder was right in his analysis of the corruption of the initiative process by big money. Maybe he, and many others, will soon realize that the proper reaction to this problem is not to stifle, limit, or reduce the use of the initiative process,

but to update and democratize it by using modern technology to make it accessible to everyone, not just those with enough money to take advantage of it in its current, vulnerable state.