Chapter V

Privacy-Sensitive Tracking of Behavior with Public Information Systems: Moving Beyond Names in a Globalizing Mass Society

Chris C. Demchak, University of Arizona, USA

Kurt D. Fenstermacher, University of Arizona, USA

Abstract

This chapter explores the roles of names and name equivalents in social tracking and control, reviews the amount of privacy-sensitive databases accumulating today in U.S. legacy federal systems, and proposes an alternative that reduces the likelihood of new security policies violating privacy. We focus on the continuing public-authority reliance on unique identifiers, for example, names or national identity numbers, for services and security instead of dissecting a better indicator of security threats found in behavior data. We conclude with a proposed conceptual change to focusing the social-order mission on the behavior of individuals rather than their identities (behavior-identity knowledge model, BIK). It is particularly urgent to consider a different path now as increased interest in biometrics offers an insidious expansion of unique identifiers of highly personal data. E-government can be wonderful for central government's effectiveness and efficiency in delivering services while

also being a disaster for both privacy and security if not regulated legally, institutionally, and technically (with validation and appeal processes) from the outset.

Introduction

For a nation, ensuring security and acceptable social order are key missions of central governments; identifying and then restraining those who act contrary to societal rules are essential to these missions. Thus, reaching back to China's Han Dynasty or William's Domesday Book in 1086, governments have developed census and other list-making activities intended to monitor compliance. As populations grew and people moved, clan, geographic, marriage, or professional affiliations slowly became names to uniquely identify individuals. Being known to a legal system by a name, however, does not mean one's behavior is known. To know one citizen or many, nations like organizations have long used names as the key tracking device, but have needed to use local surveillance by the individual's community to monitor an individual's behavior. As long as communities were relatively immobile, the name-plus-neighbors system worked sufficiently well to allow small, local police units to supplant centuries of military-based internal social control in Europe.[1]

Today, however, the emerging global mobility of the information and terrorism age has changed the parameters of governments' roles in social control, the security needs of Westernized societies, and the privacy of citizens of democratic states. To address the first two factors, some governments have lessened the third: Privacy has routinely been sacrificed for security in a perceived privacy-security trade-off. Today, the firewall of "practical obscurity unless a criminal suspect" has been massively eroded by public authorities handing out private information in the name of public openness, inadvertent community data sharing, technological oversights in releasing data, and even commercial interests and seeking data for private market purposes. The legacy systems of most governments—including state and federal agencies in the United States—have not adapted to the new circumstances, especially the increasing shortcomings of overreliance on unique, persistent identifiers such as names and Social Security numbers (SSNs) when the goal is behavior monitoring. Public information systems need a new regime that will support the changing goals of governments while preserving the privacy that citizens expect in democratic societies.

This chapter explores the roles of names and name equivalents[2] in social control, reviews what kinds of data are being accumulated today in legacy systems, and proposes an alternative focused on the security goal that reduces the likelihood of violating the privacy of ordinary citizens. We focus on the Achilles heel in the government's efforts to both ensure social order and yet minimize the loss of privacy: the continuing reliance on unique identifiers, for example, names or national identity numbers. We conclude with a discussion about a conceptual change to focusing the social-order mission on the behavior of individuals rather than their identities. Such a system variation would be an intermediate step to a world of citizens' control of their private identities while allowing traceable public behavior. It is particularly urgent to consider a different path now as increased interest in biometrics (Alterman, 2003; Barton, Byciuk, Harris, Schumack, & Webster, 2005; Boukhonine, Krotov, & Rupert, 2005; Harris, 2003; Milone, 2001; Zorkadis & Donos, 2004) offers an insidious

expansion of unique identifiers. While names and other identifiers can change, identifying an individual with an unchangeable physical attribute can transform transient mistakes into permanent ones. Moreover, if biometrics become casually linked to privately held data, it will be exceptionally difficult to return the genie to the bottle to ensure privacy at even minimal levels within or beyond our borders. The increasing use of radio technologies, such as radio-frequency identification (RFID), further exacerbates privacy and identification issues by sharing data wirelessly (Anonymous, 2006; Juels, 2006; Nisbet, 2004; Pottie, 2004; Roberts, 2006; Soppera & Burbridge, 2005).

Names Work with Less Mobile Populations

Tracking an individual's behavior begins with an identifier uniquely associated with that individual, which then serves as an index that points to a record of violations of required or proscribed behavior; traditionally, the identifier is a label permanently attached to the individual. Given the typical characteristics of social tracking schemes (listed in Table 1),

Table 1. Attributes of social tracking processes

Attribute	Attribute Definition
Direct or Indirect	Tracking is focused on the individual (direct) or on surrogate indicators (indirect), such as a criminal record or inferred crimes.
Obvious or Obscured	Tracking is apparent to those tracked through normal means, such as through sight or hearing, or by a cop on beat (obvious), or tracking is hidden from view, such as through camouflaged, remote cameras (obscured).
Ubiquitous or Selected	Tracking functions are everywhere, such as speed-limit enforcement cameras being at all intersections (ubiquitous), or tracking takes place in some places, such as cameras being only at major street intersections (selected).
Task Related or Membership Related	Tracking focuses on task-specific behaviors, such as monitoring professional activities through licensing requirements (task related), or tracking focuses on monitoring, for example, as practiced in specific religious groups (membership related).
Continuous or Intermittent	Tracking is continuous or is limited to specific periods (intermittent).
Intrusive or Nonintrusive	Tracking requires some accommodation by the observed, such as an electronic monitoring bracelet for suspects freed on bail (intrusive), or tracking requires no accommodation, such as a software-driven, embedded tag turned off simultaneously with purchase (nonintrusive).
Acknowledged or Unacknowledged	Tracking requires the individual's acceptance, such as picking up a name tag at individual events (acknowledged), or tracking is embedded routinely in all organizational activities, for example, by routinely wearing a uniform (unacknowledged).
Scalable or Fixed Data	Tracking data are easily expanded, for example, additional information may be added at will through, say, colors and patterns in clothing choices within a minority group (scalable), or tracking data are restricted to fixed inputs, such as clothing restricted to certain kinds of cloth and color choices (fixed).

name equivalents work well so long as the tracked individuals do not move frequently. In fact, when German government officials sought to prevent a further rise in the terrorism of the 1970s, they mandated extensive name gathering (and in some cases, forced name modifications) as part of the 1993 census for just this purpose—a move that upset and confused many German citizens (Benjamin, 1993). Table 1 lists many of the variations found in social tracking regimes that names or their equivalents embody.

Historically, names—which often encoded clan and familial relationships—served the purpose of labeling individuals relatively well across these characteristics. In small, relatively fixed communities, a single name sufficed for centuries; however, as populations grew and mobility increased, the need for more specificity in individual identity produced second, third, and even fourth names. With further population growth, names were augmented with clans, birth dates, birthplace names, and even occupations. Because individuals rarely moved around, they could not easily forsake their given names and so names served as early biometric equivalents. One could not simply dump the birth name of "John the miller's son" without going a long, dangerous distance from home.

In limited-social-mobility environments with few opportunities to adopt a new personal label, names are effective tracking mechanisms. These labels are usually direct, ubiquitous, and durable. All people have a name given directly by their parents. If the person is socialized into sharing this label on social encounters, the name becomes widely known in small societies. Once a name is taken for granted, it is also usually nonintrusive and generally unacknowledged. Even if initially rooted in an occupation, names eventually become membership-tracking mechanisms; John the Miller has a great-grandson named Joseph Miller, who may well work as an optometrist. In some groups, people carry multiple middle names to allow more distinct identification and familial affiliation, as with the patronymics common in many societies. Moreover, names are durable in the sense that even a person in a coma continues to hold her name; names are thus well suited for use in continuous tracking processes. Because all modern societies are rooted in histories in which names (or their equivalents) worked well for social tracking, they have continued as a popular choice for government tracking to this day—even when they may no longer be appropriate.

Static Name Equivalents Dominate Governmental Systems

Managing the descriptive data defining an individual, society, or subordinate group in modern governance means enormous influence over the social options available to the individuals or groups. For example, being able to categorize who is and is not unemployed has been a longstanding political struggle in the United States. During the political debate surrounding the formation of the Department of Labor at the turn of the 20th century, conservative business elements succeeded in making the new cabinet-level department weak and ineffectual by deliberately keeping the Bureau of Labor Statistics out of the new department. Without the ability to control the lists of who is and is not employed, the department was routinely unable to win legislative battles critical to its institutional and political influence. The labor department is known to be one of the least influential departments of the cabinet (Kimeldorf & Stepan-Norris, 1992). In another example, the small religious party Shas of Israel demanded the Ministry of Education post in any alliance government. In this role, the Shas minister could define the terms under which hundreds of religious Israelis could be

classified as students. By consistently labeling Shas members as such, the central government supported them modestly for most of their lives through several simultaneous scholarships. (The leader of the Shas eventually went to jail for fraud for issues related to the practice of counting every three credit hours as full-time religious study, enabling each student to get three scholarships at once [Amado, 2001]. The scholarships, however, did not cease following the leader's arrest—the labels stuck.)

The Emergence of Name Equivalents

As the size of societies has grown, however, name equivalents have emerged to augment and sometimes replace birth names. Surnames alone are too variable in spelling and too often duplicated to support effective tracking in modern mass societies with redistributive functions like welfare or national income taxes. Furthermore, names in immigrant communities are often simply what the new immigrant says it is. With easily changed or lost papers, names as identifiers become less and less accurate. Names easily change at borders—often shortly before border officers ask for one. Linguistic differences mean names can be misunderstood, profoundly affecting the lives and social acceptance of those whose names are altered. The relative immutability of names in the Westernized world contrasts sharply with the fluidity of names from Middle Eastern cultures. While family and clan associations are not usually flexible, what a person calls himself varies according to his internal version of his life's progress (Peteet, 2005). This tendency is not a problem in relatively immobile societies because other members of the society can identify the individual and recall his various names if asked.

In the globalizing, more mobile world, however, name fluidity causes routine identification difficulties for passport officers, a difficulty exploited by those operating covertly across borders. American families have many stories of a grandmother's familial name changing upon entry into the United States as an immigrant. In an informal interview, a colleague explained that an Ellis Island immigration official changed his Catholic Hungarian family name into a historically Jewish name in the 1930s. The family story is that the officer could not pronounce the immigrants' birth name and generously wanted to help the family out by giving them a good "American" name. In so doing, the officer changed the way the whole family was accepted within New York City's largely Jewish Bronx borough for the next two generations.

Altering a name is often enough more than a mistake or a convenience. In modernizing nations, changing clan or religious affiliations can mean the difference between survival and starvation. In several small eastern Indian states bordering the largely Muslim country of Bangladesh, a remarkable preponderance of Christians exists in the data files of public authorities. Being Muslim in Hindu India and an illegal immigrant is a double burden for those filtering into India from Bangladesh for economic survival. A Bangladeshi Muslim could not easily pass as Hindu but could pass as a Christian, the now dominant political elite in these smaller states. Hence, illegal immigrants declare themselves to be Christians to be accepted. They must also change their Muslim given names, not only for acceptance but also for physical safety since the Koran authorizes all Muslims to kill at will any Muslim who has converted. The story becomes more complex if they attempt to go home for a visit. They need to seamlessly shed the new names and trappings for a while, and then resume them

without calling attention to themselves once back in India. The frequent name changes can cause a good deal of confusion for both Indian and Bangladeshi border authorities (Indian Press Trust, 2005).

National Identification Numbers

In the middle of the past century, for most of the Westernized world, identity cards with names and often with numbers (the Social Security number in the United States) began to be employed to identify a country's nationals, not always for the best of purposes. The first nationwide national identity number in France was issued by the Vichy government in 1940 to help identify Jewish French citizens intended for deportation to Germany (Wikipedia, 2006). In smaller Western nations with a relatively homogeneous and immobile population, such as Sweden, the national identification number (*personnummer*) encodes an individual's date of birth and sex along with a digit sequence and a checksum (Riksskatteverket, 1999). In the much larger, immigrant-fed, decentralized United States, SSNs are allocated by region and so the number reveals (indirectly) the postal code of the application's origin, which might or not be the birthplace of the applicant. In both instances, the number is meant to provide singularly identifying tracers, which, when linked to other distinctive data, provide the authorities with the information needed to make allocation decisions across the society. For example, Britain issued, in both world wars, national identity cards to ease rationing that were then discarded after the wars. National identification numbers are not universal but, along with the biometric passport, are gaining popularity due to the terrorism threat from visiting or immigrant populations. Even Britain will have a mandatory national identity card for all its citizens by 2013; today, 21 of 24 members of the European Union have some form of identity card, though not all centrally managed (Wikipedia).

Collection of Privacy-Sensitive Data by the United States Government

The use of a name and an associated number as tracking mechanisms has grown across agencies and nations. In the United States, for example, it is difficult to estimate the total number of databases across state and federal agencies that collect and use privacy-sensitive data on citizens, almost always associated with a name and/or the ubiquitous Social Security number. The 1974 Privacy Act (5 U.S.C. 552a, Public Law 93-579) requires agencies of the federal government to report annually on what files they maintain that may have privacy implications and the rules by which the data was accumulated. Searching online through http://www.fedgov.gov, however, it is difficult to find more than a smattering of these agency filings. Announcements of these file holdings must be published in the Federal Register as Privacy Act notices; since 1995, the notices have also been published online at the U.S. Government Printing Office's Web site (*GPOAccess*, http://www.gpoaccess.gov/privacyact/index.html; U.S. Government Printing Office, 2004). However, visiting *GPOAccess* does not easily provide compilations across agencies; rather, the entries tend to be annual, dated, and inconsistent—several of the links to agency files were broken with no alternative link provided.

Despite the difficulty in accessing these lists, government agencies do host a wide variety of privacy-sensitive databases, some of which are listed online. The Department of Defense listed in 2003 that it had 166 such databases across 19 subagencies, including each of the major services. The latest list available for the Department of the Interior was published in 2001 and listed 95 privacy-sensitive databases. Other agencies with compilations noted are large and small. For the year 2002, the Tennessee Valley Authority said it had 29 such databases while the Railroad Retirement Board said it had 33 privacy-sensitive files in 2003. The oldest list came from the Fish and Wildlife Service, dated 1992, which noted roughly 40 distinct databases, while a list for the Commodities Futures Trading Commission dated 1999 also listed about 40 privacy-sensitive collections. Many lists have no discernible year and are quite large. For example, the Department of Interior claims 191 privacy-sensitive collections, but there is no year given. Similarly, the Office of Personnel Management notes it has 39 privacy-related databases, but no year is provided (U.S. Government Printing Office, 2004).

Complicating an effort to estimate the breadth of the holdings in the federal government are the waivers and exemptions taken by the agencies. Very often, a posted Privacy Act notice concerns the intent of the agency to not discuss the contents of a database. For example, the Transportation Security Administration (TSA) notes that it had roughly 15 privacy-sensitive databases (U.S. Government Printing Office, 2004), including several it had just added. However, the bulk of the discussion explained why the TSA did not list what private data were actually collected in that database for reasons of national security. It is instructive to note that not only are these filings difficult to locate and document conveniently online, but the most precisely dated and cumulated lists are older, predating the current post-9/11, security-conscious policy environment.[3]

Another way to gain an appreciation of the magnitude of the growing personal data banks held by public authorities for a variety of reasons is to look at databases in terms of communities. For example, in the days of paper, applicants for jobs, grants, or consulting contracts would provide personal data that eventually were discarded to save space. Those not hired, awarded, or selected would certainly have their data cleansed from the system periodically. That an application is rejected today is no guarantee that all that data did not go into several general digital files easily stored and shared inside an agency or among agencies. In Congressional hearings in late 2004, for example, the Congress was told that 80% of all applicants for positions in the federal government were submitting applications online, directly into databases.

Being a mere contractor is no protection. In the same hearing, the representative of the National Science Foundation (NSF) said 100% of grant proposals were now digitally submitted and processed, including not only personal data on the principal investigating professors but also on associated scholars, consultants, and often graduate students. For job applicants and individuals associated with an NSF grant application, the physical firewall created by paper applications and dispersed filing cabinets accumulating personal data has vanished; moreover, there is no particular information on where else that data might migrate to or for what other purposes that exceptionally personal data might be used (U.S. House of Representatives, 108th Congress, 2004).

Regional Government Data Collection

State or provincial governments make the threats more complex as well. In the United States, even if state governments have only a fraction of the inventory of privacy-sensitive databases held by the central government, there are still another 50 complex, multilevel entities collecting data on individuals who reside, work, or request any kind of service in the state. Beyond the state level are still more counties, cities, and even public-utility districts. Today in the city of Tucson, Arizona, a local city policy to combat the methamphetamine epidemic now requires ordinary purchasers of any over–the-counter medicine containing pseudoephedrine to fill out a form giving personal identifying data. Who receives, transcribes, stores, and then uses that data is not clear, but no purchase is authorized unless the data are surrendered. This sign-in-before-you-buy policy is spreading across the United States (Colker, 2005) in an otherwise admirable effort to stop the methamphetamine epidemic sweeping the country's teenagers, but it squarely and unrestrictedly places otherwise private data in the unprotected files of hundreds of pharmacies across the same locations.

In a Mobile, Digitized World, "Practical Obscurity" No Longer Saves Privacy

For most of the 20th century, the effort to amass privacy-sensitive data was expensive and time consuming. Citizens and public authorities endured fragmented policies and paper-based or proprietary databases dispersed across states, counties, jurisdictions, and departments within agencies. Policies were often inconsistent across states and agencies, even when data collection was driven by national initiatives mandating consistency such as aid-to-dependent-children programs or the sharing of gang-related data across police agencies. Furthermore, increasing mobility exacerbated the accuracy of social tracking by names or name equivalents; population movements tended to reinforce the practical difficulties of accumulating data on many people at once. Privacy was thus assured simply because people could move easily but personally revealing data about them could not.[4]

Two global trends converged in the late 1990s to make legacy systems less useful while simultaneously trading off privacy without a commensurate, but expected, improvement in security. First, the widespread and enthusiastic embrace of easily exchanged digital data leapfrogged the normal processes of social and legal adjustment. Over just a few years, public authorities across the Westernized world moved rapidly from cumbersome paper or platform-bound legacy files to the easily distributed and accessible data hoards, seeking unprecedented benefits and unleashing unforeseen threats. Second, a now clearly globalizing social movement has emerged to pursue an ancient "war of a thousand strikes" from within the normal operations of increasingly heterogeneous Westernized societies (writ large) and the United States and allies in particular. In response, the United States and other Westernized nations are moving to restrict privacy to find terrorists. The first government trend inadvertently sacrifices privacy; the second deliberately reduces personal privacy in hopes of preempting catastrophic violence in Western communities.

Abuse of Personal Information

Beyond governments and terrorists are commercial entities in corporations and criminals, all seeking to gain some monetary advantage from an individual's personal information. Today the commercial world is collecting data at a previously unimaginable rate and making the results available to anyone willing to pay for access. Credit reports are regularly sold to businesses but little is done to control what happens to those reports once delivered. In 2004, investigators for the Social Security Administration (SSA) arrested a former manager of a local furniture store using stolen credit reports from the store's credit clients to conduct elaborate frauds involving consumer loans worth hundreds of thousands of dollars, according to the testimony of Patrick P. O'Carroll of the SSA (U.S. House of Representatives, 2004).

However, it is the unprecedented presence of American public records on the Web, open not only to citizens but also to the wider world, that offers criminal access into the private lives, finances, and future prospects of individuals in the United States. The easy complacency borne of an era of fragmented, hard-to-find databases made acceptable this rush to accelerate connections across previously unconnected databases with private citizen information. It tends to come as a shock to most citizens when they find out just how easily they are completely identifiable by databases now offered openly. For example, the abused wife who bought her own house 5 years ago might find today that her purchase information, including her new home address, is now online courtesy of her local county tax assessor. In the intervening 5 years, county records were neatly archived digitally and published with nearly no effort to protect privacy since they were, often by law, "public" records. For most of these newly published county records, there is no log of who reads them, who copies the data, or even who spends hours searching and collating hundreds of those records. Instead, these data are simply tossed out in cyberspace for human and software collectors to gather, sell, or use for any purpose.

Identity Theft

The result for the United States is an extraordinary rate of identity theft, phishing attacks (whereby victims are lured into entering personal information on online forms that masquerade as legitimate enterprises), and other crimes enabled by this wealth of private information. In 2004, investigators for the Social Security Administration were startled to see an advertisement on an online auction Web site offering about 250,000 Social Security numbers for sale. The individual had pilfered them from the files of a large state university that used Social Security numbers to track students, staff, and contractors (U.S. House of Representatives, 2004). In such thefts, the costs are rarely calculated, but across all categories, it is millions of dollars and senseless losses in time and lives disrupted.

Balancing Privacy and Social Control

The difficulty for a government in addressing the situation is defining the correct balance in ensuring social control. How far should public authorities be able to intrude into private

identity in order to enforce rules in a mass society? What compensating policies and sanctions are required to ensure a remaining firewall of individual protections of privacy-sensitive data? Governments do need to accumulate data on citizens to analyze mass trends to set the nation on better paths for future prosperity. Security forces do need to track down violators of the social order quickly and firmly, within the rule of law. Businesses do need a way to anticipate consumer wants and prepare in advance to meet those evolutions in needs and desires. However, the digital frontier transferred the convenience of access from the small pool of visitors to local public-records archives to the world beyond our borders without pause to consider what to protect and what was not necessary to share with, say, sociopaths. A good example of this lesson not learned is the MySpace Internet community (http://www.myspace.com) that encouraged youngsters to meet online, only to discover pedophiles took the opportunity as well. The system is not designed to keep these predators from lying about their age and luring credulous youngsters into private chats (Rawe, 2006). As a result, the openness and convenience of MySpace is now strongly constrained by the Web site owners seeking protection from lawsuits and from parents now concerned about a previously unheard of vulnerability for their children.

The abrupt rise in Web-available data has parallels with the historical shift in the United States from the frontier communities of the early Tennessee Valley, where surviving depended on skill and luck, to the frontier communities of gold-rush California, where schools, prostitutes, opium dens, murderous fights, libraries, and duplicitous storekeepers sat beside one another. The difference is ease of access to one's private life. Now both governments and criminals across layers and layers of unaccounted-for name-based intermediary and invisible databases can reach out to touch or disrupt citizens. E-government (known as i-government in Europe) can be a wonder drug for central government's effectiveness and efficiency in delivering services while also a disaster for both privacy and security if not regulated legally and physically (with validation and appeal processes) from the outset.

Track Actions, Not Labels

"[A]nonymity and pseudonymity are not all-or-nothing qualities but can be achieved in degrees and through layers of cloaking" (Nissenbaum, 1999, p. 144).

In a mobile, digitized, globalizing world, neither security nor privacy is ensured by simply linking legacy systems more efficiently. Names and labels say only who someone is, not what they are doing; in other words, they convey status but not action. In a world that demands preemption of bad behaviors for security but also asks for the protection of privacy, names are no longer good even as a primary point of reference. Security threats come from behaviors, and names are poor behavior-tracking mechanisms. They are only useful if public security forces already using other behavioral monitors separately monitor individual actions. However, names, national identity numbers, birth dates, and addresses freely handed out in the wild function well as attractors of criminal behaviors. Thus, using identity as a first choice in tracking terrorist behavior fails to pinpoint the bad actors for security purposes but handily exposes citizens' private lives to other kinds of criminals. If security requires a focus on behavior and privacy requires a firewall around critical personal identities, then a different conceptual approach is necessary, one that emphasizes the tracking of undesirable behavior over tracking a name.

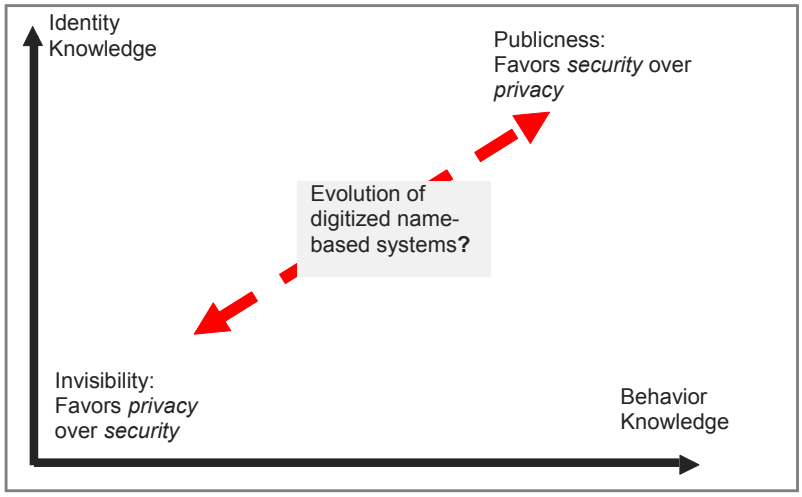
To balance security and privacy but retain the tradition and advantages of names, one needs not an absolute name but a conditional one—one that becomes a true name only upon triggering behavioral signals of public interest. In short, the alternative behavior-based policy would produce identifying information much like names but would mask the real name, birthplace and birth date, national identity number, home address, and maiden name for the sake of privacy. This new identifier (a pseudonym, rather than a true name) would, like names in the less mobile era, be direct, ubiquitous, and durably connected to an individual's true identity. With the issue of a new identifier, we could enable a new tracking mechanism that would be (usually) nonintrusive, unacknowledged, membership specific, and scalable. The relative obviousness of the mechanism would vary according to the circumstances. A practical alternative to the current regime would replace a name for the purposes of public tracking until the name becomes necessary for public threat reduction.

A system of traceable pseudonymity seems the most promising alternative if it can be seamlessly inserted into the existing structure of societal interactions that currently provides all this freely floating data. A looming current difficulty is the growing use of uniquely identifying biometrics. Shortly after the September 11th attacks, a car-loan agency was reported to have required fingerprints, a critical biometric, from customers before they were allowed to rent cars (Scheeres, 2001). Disney theme parks—purportedly the happiest places on earth—now require finger scanning for park admission (Local 6 News, 2005). An alternative behavior-based system of monitoring is urgently needed before all these loosely secured databases become linked equally freely to immutable individual biometric data carried around on, say, easily read credit-card magnetic strips.

The behavior-identity knowledge (BIK) system (Demchak & Fenstermacher, 2004a, 2004b, 2005) begins conceptually with the notion that private data are kept by the owning individual and masked for public consumption by a trusted third party (TTP). The TTP is envisioned as a nonprofit, networked group of institutions that use technical and social engineering to secure critical data. The TTP would maintain the linkage between an individual's masked identity (associated with one or more pseudonyms) and the individual's true identity. The system would depend on a public-key infrastructure (Adams & Lloyd, 1999) or PKI. A PKI builds on the notion of public-key cryptography (Salomaa, 1996), which uses two complementary, numeric keys to encrypt and decrypt information. One key is known to all participants and so is labeled the public key; the second key is known only to its individual owner (and, in the BIK world, to the TTP) and so is called the private key. A system can encrypt data with either the public or private key and the encrypted data can then only be decrypted with the complementary key. Chaum (1992), Chaum and Evertse (1987), and Chaum (1981, 1987) describe in detail how a PKI can be used to support data privacy in a BIK-like world.

In a BIK world, a person would access a secure portal, perhaps at his or her local motor-vehicle office, to use a private key—known only to the person and the TTP—to create a masked identity, which is then used for all public interactions such as making purchases or presenting credentials. The needed information is encoded on a smart card, a more secure version of the widely used magnetic-stripe technology currently used for credit and debit cards. Smart cards have been studied extensively for their advantages in protecting personal information while supporting more advanced transactional infrastructures (Bailey & Caidi, 2005; Banaszak & Rodziewicz, 2004; Bolchini & Schreiber, 2002; Chan, Chanson, Ieong, & Pang, 2000; Fan, Chan, & Zhang, 2005; Yang, Han, Bao, & Deng, 2004). Biometrics are also encrypted, used only to verify that the individual offering the smart card is the individual

Figure 1. BIK framework



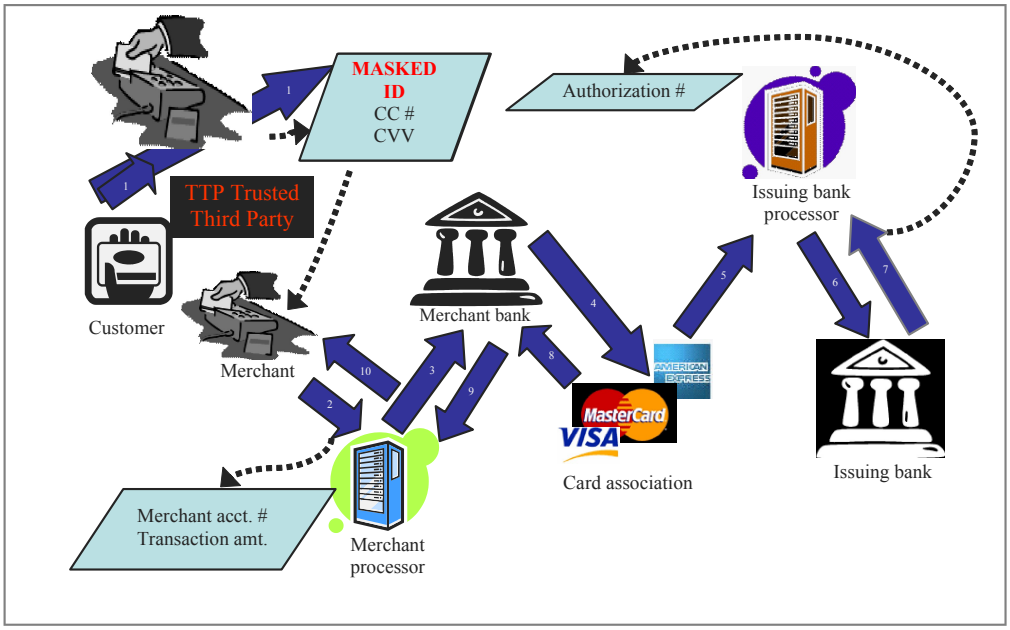
behind the masked identity; biometric data are never stored away from the TTP or on a particular card. The masked data are then collected just as data are today with an additional data storage site at the TTP. This is further made anonymous for sale to commercial entities who receive only aggregate data, saving them the need to pursue databases at the individual level and preserving the individual from the tricks of the commercial world to winnow out personal data; Figure 1 portrays this alternative.

In this system, only patterns of behavior, not names, elevate a masked identity out of the crowd for further inspection by authorities. Under legally prescribed conditions, authorities then must validate the accuracy of the linkage between the behavior and the masked identity and then request of the TTP information on the true identity of the citizen. In this process, much stricter legislation on the collection, storing, and use of true personal data will be necessary.

Over time, the current static identifying data of name-equivalent legacy systems become useless as the world changes but legacy data does not. For example, because Americans move on average every 2 years; the John Doe who was living on 1st Street may or may not be the 264735BBB living in the neighborhood now. The identity data now in the wild become less and less useful as the masked identity slowly becomes disconnected from previous uncontrolled databases commercially and publicly. Behavior data, however, are more easily available to both government and legitimate commercial entities, with true identities hidden behind technical, institutional, legal, validation, and appeal requirements. Figure 2 demonstrates how BIK blends into the current credit-card transaction infrastructure.

While the BIK model does not solve all the issues of privacy and security trade-offs, it has in principle the advantages of fitting relatively seamlessly into existing systems. It could well offer an intermediate step to a world of citizen control of their private identities while allowing traceable public behavior to ensure security against terrorism and other globalizing threats.

Figure 2. Living in a BIK world



References

Adams, C., & Lloyd, S. (1999). *Understanding public-key infrastructure: Concepts, standards, and deployment considerations.* Macmillan Technical Publishing.

Alterman, A. (2003). "A piece of yourself": Ethical issues in biometric identification. *Ethics and Information Technology, 5*(3), 139.

Amado, R. (2001). Checks, balances, and appointments in the public service: Israeli experience in comparative perspective. *Public Administration Review, 61*(5), 569-584.

Anonymous. (2006). MIT and HID to address RFID privacy concerns. *Sdm, 36*(5), 40.

Bailey, S. G. M., & Caidi, N. (2005). How much is too little? Privacy and smart cards in Hong Kong and Ontario. *Journal of Information Science, 31*(5), 354-364.

Banaszak, B., & Rodziewicz, K. (2004). Trust and security: Digital citizen cards in Poland. *Electronic Government, 3183*, 342-346.

Barton, B., Byciuk, S., Harris, C., Schumack, D., & Webster, K. (2005). The emerging cyber risks of biometrics. *Risk Management, 52*(10), 26.

Bayley, D. H. (1975). The police and political development in Europe. In C. Tilly (Ed.), *The formation of national states in Western Europe* (pp. 328-379). Princeton, NJ: Princeton University Press.

Benjamin, D. (1993, July 15). What's in a name greatly interests German officialdom. *Wall Street Journal*, p. 1.

Bolchini, C., & Schreiber, F. A. (2002). Smart card embedded information systems: A methodology for privacy oriented architectural design. *Data & Knowledge Engineering, 41*(2-3), 159-182.

Boukhonine, S., Krotov, V., & Rupert, B. (2005). Future security approaches and biometrics. *Communications of the Association for Information Systems, 16*, 1.

Chan, P. N., Chanson, S. T., Ieong, R., & Pang, J. (2000). Smart card payment over Internet with privacy protection. *Smart Card Research and Applications, 1820*, 98-104.

Chaum, D. (1992). Achieving electronic privacy. *Scientific American, 267*(2), 96-101.

Chaum, D., & Evertse, J. H. (1987). A secure and privacy-protecting protocol for transmitting personal information between organizations. In *Advances in Cryptology—CRYPTO '86: Proceedings* (LNCS 263, pp. 118-167). Springer-Verlag.

Chaum, D. L. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM, 24*(2), 84-90.

Chaum, D. L. (1987). *Security without identification: Card computers to make big brother obsolete.* Retrieved May 10, 2006, from http://www.chaum.com/articles/Security_Wthout_Identification.htm

Colker, A. C. (2005). Restricting the sale of pseudoephedrine to prevent methamphetamine production. *NCSL Legisbrief, 13*(7), 1-2.

Demchak, C. C., & Fenstermacher, K. D. (2004a). *Balancing security and privacy in the 21st century.* Paper presented at the Second Conference on Intelligence and Security Informatics, Tucson, AZ.

Demchak, C. C., & Fenstermacher, K. D. (2004b). Balancing security and privacy in the information and terrorism age: Distinguishing behavior from identity institutionally and technologically. *The Forum, 2*(2), Article 6.

Demchak, C. C., & Fenstermacher, K. D. (2005, September). *Ensuring security, enhancing privacy.* Paper presented at the Eighth Public Management Research Conference, Los Angeles.

Fan, C. I., Chan, Y. C., & Zhang, Z. K. (2005). Robust remote authentication scheme with smart cards. *Computers & Security, 24*(8), 619-628.

Harris, S. (2003). Biometrics need a measure of security. *Government Executive, 35*(9), 70.

Indian Press Trust. (2005). *"Abnormally high" growth of Christians in NE.* Retrieved August 1, 2006, from http://www.expressindia.com/fullstory.php?newsid=41957

Juels, A. (2006). RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications, 24*(2), 381-394.

Kimeldorf, H., & Stepan-Norris, J. (1992). Historical studies of labor movements in the United States. *Annual Review of Sociology, 18*, 495-517.

Local 6 News. (2005). *Finger scanning at Disney parks causes concern.* Retrieved August 1, 2006, from http://www.local6.com/news/4724689/detail.html

Milone, M. G. (2001). Biometric surveillance: Searching for identity. *The Business Lawyer, 57*(1), 497.

Nisbet, N. (2004). Resisting surveillance: Identity and implantable microchips. *Leonardo, 37*(3), 210-214.

Nissenbaum, H. (1999). The meaning of anonymity in an information age. *The Information Society, 15*(2), 141-144.

Peteet, J. (2005). Words as interventions: Naming in Palestine-Israel conflict. *Third World Quarterly, 26*(1), 153-172.

Pottie, G. J. (2004). Privacy in the global e-village. *Communications of the ACM, 47*(2), 21-23.

Rawe, J. (2006). *How safe is MySpace?* Retrieved from http://www.time.com/time/archive/preview/0,10987,1207808,00.html

Riksskatteverket. (1999). *Personnumer (SKV 704)*. Retrieved July 31, 2006, from http://skatteverket.se/download/18.b7f2d0103e5e9ecb0800074/70407.pdf

Roberts, C. M. (2006). Radio frequency identification (RFID). *Computers & Security, 25*(1), 18-26.

Salomaa, A. (1996). *Public-key cryptography.* Springer.

Scheeres, J. (2001). *No thumbprint, no rental car.* Retrieved July 30, 2006, from http://www.wired.com/news/privacy/0,1848,48552,00.html

Soppera, A., & Burbridge, T. (2005). Wireless identification privacy and security. *BT Technology Journal, 23*(4), 54.

U.S. Government Printing Office. (2004). *Privacy Act issuances: About.* Retrieved July 31, 2006, from http://www.gpoaccess.gov/privacyact/about.html

U.S. House of Representatives, 108th Congress. (2004). *Electronic government.*

Wikipedia. (2006). *Identity document.* Retrieved from http://en.wikipedia.org/wiki/Identity_document

Yang, Y. J., Han, X. X., Bao, F., & Deng, R. H. (2004). A smart-card-enabled privacy preserving e-prescription system. *IEEE Transactions on Information Technology in Biomedicine, 8*(1), 47-58.

Zorkadis, V., & Donos, P. (2004). On biometrics-based authentication and identification from a privacy-protection perspective: Deriving privacy-enhancing requirements. *Information Management & Computer Security, 12*(1), 125.

Endnotes

1 It is rarely recognized how recently most Westernized states were internally stable enough to create police forces rather than use military units to control the internal peace. The 18th century saw the emergence of the community police force while military units focused more on outside threats. (Bayley, 1975)

2 Name equivalents are also known as "isonames" or by the Latin, "isonym."

3 The U.S. Internal Revenue Service is excluded from this discussion because it has long been known that taxpayer data is routinely transcribed from paper to digital files and the advent of online filing merely transfers the locus of data entry. Furthermore, regulations regarding the use of that data are much better established than the growing number of other databases scattered across other agencies.

4 The scope of this piece does not allow a comparison of the relative mobility of European citizens versus Americans and its impact on privacy, but a piece linking privacy, mobility, and convergence or divergence in U.S.-Europe data and privacy policies is planned for the future.

Chapter VI

E-Government:
An Overview

Shannon Howle Schelin, University of North Carolina at Chapel Hill, USA

Abstract

Information technology has fundamentally altered many aspects of daily life, including interactions with the government. The role of the Internet continues to increase as more citizens use it to find pertinent information, purchase goods and services, and participate in virtual communities. By capitalizing on the Internet revolution, governments can create new channels of communication and new methods for participation via e-government. The changing environment, coupled with citizen and business demands, encourages government involvement in e-government initiatives and related uses of information technologies. Clearly, the role of information technology in the public sector has changed rapidly over the past decade. The computer systems that were once a luxury investment for wealthy states and local governments are now supporting almost every function of local government. In virtually all local governments across the nation, information-technology investments are becoming an increasingly important area of attention for elected officials and administrative leadership alike.

Technology-Enabled Government

The public sector has made incredible strides in technology over the past decade. The investments in IT have brought the many states, counties, and municipalities into standing with other leading private-sector companies across the nation. In virtually every governmental jurisdiction, information technology is playing a vital role in each department and function of the organization. In fact, while information technology only comprised between 1 and 3% of the general fund budget, on average, the technology investments support approximately 98% of the work conducted by governments. In order to assist the public sector in moving beyond the status quo and leveraging technology as a means of delivering more efficient and effective services, as well as to maintain and gain a competitive economic-development advantage, it is important to recognize the positive technological advancements that have made significant impact on service delivery over the past 6 years. By establishing this strong technological foundation, many governments are poised to reap the rewards associated with greater investment in technology.

The scope of technology in governments across the United States can be grouped into three basic categories: infrastructure, hardware, and applications. The first two categories have seen a plethora of growth as states, counties, and municipalities have installed various communication media to assist with connecting disparate locations. One common infrastructure and hardware solution across many states has been the installation of fiber between government facilities or around jurisdictions. Other governments have chosen to use wireless technologies to connect remote locations without physically laying fiber. As service becomes less location dependent, it is essential for government employees and off-site departments to have high-quality, secured access to records and databases. Fiber-ring and secured wireless initiatives have provided a critical first step to this effort.

Another major technological impact has been generated by the powerful communication medium of e-mail. Using e-mail technologies as collaborative tools, employees are able to generate significant cost savings by the reduction of travel time for communication purposes. E-mail and other electronic communications media, such as instant messaging, allow almost instantaneous communication across departments, jurisdictions, and states and have been credited with quicker problem resolution, increased data sharing, and easier information and personnel access. Furthermore, the use of e-mail has significantly improved citizen relationships by allowing another channel of communication.

The third important technology investment is a World Wide Web presence. By creating and maintaining an outstanding Web site, cities and counties have been on the cutting edge of citizen, visitor, and business engagement. In fact, many economic-development experts indicate that a high-quality Web presence is the most important tool in a local government's development efforts (Horrigan, 2003). The National Governor's Association and the National Conference of State Legislatures offer publications concerning the value of technology investments and impact on economic development. Furthermore, Web sites provide a unique and timely vehicle for communication with citizens and visitors alike. It is an essential feature in any local government.

A final critical technological impact has been garnered through the investment in geographical information systems (GISs). The use of GIS greatly enhanced the work of local governments. For example, GIS has improved internal government efforts by aiding in meter and pipe

location. It has improved the efforts of planning departments by enabling staff members to access a comprehensive database that spatially represents areas and items of interest. In addition, GIS is one of the most productive and useful tools in technology revolution. The power and breadth of the software is being used in crime fighting, fire fighting, and countless other ways.

Most public-sector entities have seen an incredible amount of change over the past decade. Many have progressed from nontechnical to successful, technology-friendly governments with many of the investments previously mentioned. However, some governments have only recently begun to invest or consider investing in technology. These smaller or more financially challenged governments have faced a variety of issues but have created unique opportunities to leverage existing infrastructure and assets.

The term *digital divide* was originally coined to describe the division between economic groups regarding access to information technology. However, there is another type of digital divide facing governments. The majority of rural counties and municipalities in many states are experiencing significant economic hardships. These local governments are strained for the basic resources and investments in information technology are not deemed mission critical. Therefore, the gap between the technological haves and have-nots in local governments is widening.

One interesting solution to this governmental digital divide is being pioneered in small communities throughout the nation. The use of cross-boundary collaboration has become a best practice among economically strained local governments. In the collaborative model, local governments partner together in an attempt to leverage demand aggregation, economies of scale, and staff capacity enhancement in the technological arena. For example, demand aggregation can occur when a county offers a centralized procurement process that includes its municipalities in order to increase the overall value of the bid or order while enhancing the negotiating power of the governments. In order to capitalize on economies of scale, counties may seek to share IT staff on a rotational model, which allows for increased technical capacity due to greater monetary incentives.

The current economic stress facing the states mandates that new models be employed in order to address the gaps in service delivery, and cross-boundary collaboration is one such model.

There are numerous ways to invest in public-sector information technology. Some of the most common investments are focused on electronic communications and department-specific applications. However, new cross-departmental, and even cross-jurisdictional, efforts are beginning to emerge. These efforts follow the trends in the private, federal, and state sectors and create greater value for the strategic investments.

Trends

A variety of management trends have occurred in the last few years related to information-technology adoption and implementation in the public sector. This section highlights some of the most critical trends, including the advent of e-government and the move to

enterprise-wide technology efforts. Both of these trends offer significant advantages to citizens, businesses, employees, and visitors. In addition, the trends have proven to generate cost savings, increased efficiencies, and greater effectiveness in a variety of cases. The final trend explored is the advent of the chief information officer (CIO) and the increasing professionalism of the role of information-technology staff.

E-Government

E-government (electronic government) has become a buzzword in local, state, and federal government. The era of e-commerce and e-business began with the widespread adoption of the Internet in the mid-1990s and today many citizens expect the same responsiveness and access to government services as found in the private sector. Not only are citizens looking for improved ways to interact with the government, elected officials demand improved services to enhance their legacies. Competitive governments do not want to be seen as slow adopters of e-government (Sprecher, 2000).

E-government has become a mainstay in local, state, and federal government. According to the 2004 International City and County Managers Association (ICMA) e-government survey, over 91% of municipalities with populations larger than 2,500 have Web sites, compared to 73% in 2002. In North Carolina local governments, the Center for Public Technology has found that over 80% of all local governments have Web sites and more governments are developing a Web presence each month. Additionally, the 2003 Pew Internet and American Life Project (Horrigan, 2003) indicates that 77% (97 million people) of American Internet users have accessed at least one governmental Web site. Not only are citizens looking for improved ways to interact with the government, but elected officials demand improved services to enhance their legacies.

Although there is widespread interest in the topic, e-government lacks a consistent, widely accepted definition. It is often related to revolutionizing the business of government through the use of information technology, particularly Web-based technologies, that improve internal and external processes, efficiencies, and service deliveries. The American Society for Public Administration (ASPA) and the United Nations Division for Public Economics and Public Administration (UNDPEPA) have defined e-government as "utilizing the Internet and the world wide web for delivering government information and services to citizens" (UN & ASPA, 2001). Based on this working definition of e-government, this chapter seeks to examine the theoretical constructs, historical premises, and associated typologies of e-government.

Historical Premises

E-government has evolved from the information-technology revolution. Information technology enables new methods of production, increases the flow and accuracy of information, and may even replace traditional standard operating procedures (Landsbergen & Wolken, 2001). Information technology in government has long been acknowledged as a method for improving efficiency and communication (Kraemer & King, 1977; Norris & Kraemer, 1996). However, until the advent of the Internet, the use of technology in government primarily

dealt with the batch processing of mass transactions using mainframe computers. Now, IT developments such as electronic mail (e-mail) have changed interpersonal communications to eliminate the constraints of geography, space, and time with profound organizational consequences (Rahm, 1999). The ability to buy and sell goods and services via the Internet has led to new private-sector industries, constituting a new business model that the public sector now seeks to emulate. In addition, IT has promoted globalization, which also changes the environment within which public agencies function (Kettl, 2001).

The main concerns of e-government now focus not only on the electronic dissemination of public information arising from traditional agency functions, but even more on reinventing agency processes to fully exploit the potential of information technology. As Fountain (2001) has noted, the reinvention process requires overcoming the rigidities and limits of traditional bureaucratic forms. Specific objectives may include the centralization of public data and the improvement of internal processes and communications (Alexander & Grubbs, 1998).

In detailing the history of e-government, it is important to note the distinctions between public-sector usage of information technology and e-government initiatives. Although there is a distinction between public-sector information technology and e-government, they are often interdependent and difficult to quantifiably separate, but e-government is that subset of public information technology that involves the delivery of government services and information to citizens, as defined by UN and ASPA (2001). This delivery of services and information also involves the integration of government networks and databases to allow for cross-agency communication and interaction, which is an internal technology application (Moon, 2002).

One of the first comprehensive visions of e-government is found in the 1993 National Performance Review report, *Creating a Government that Works Better and Costs Less: Reengineering Through Information Technology* (Gore, 1993; Kim & Wolff, 1994). This report laid the groundwork for new customer- and client-oriented ways for agencies to engage citizens via technology, involving both improved agency processes and improved methods of delivery. Most reinventing-government literature has cited the need to rely on information technology to improve citizen-centric government services (Kettl, 1998; Osborne & Gaebler, 1992). It is common for current works to refer to the symbiotic relationship between the earlier reinventing-government movement and the current e-government movement (Ho, 2002; Scavo & Shi, 2001). Although the two movements are conjoined, the prospects are that the focus of public administration on e-government will endure for the foreseeable future, outlasting the reinventing-government movement.

The 1995 amendment of the 1980 Paperwork Reduction Act (PRA) was another important milestone in the history of e-government. This amendment offered specific policies on issues associated with managing electronic information, including the establishment of standards, mandates for cross-agency information-technology initiatives, and technology investment guidelines (Relyea, 2001). By outlining guidelines for information technology, the amended PRA solidified the government's commitment to improving citizen services via new channels based on technology. Several other pieces of federal legislation focusing on information technology and e-government followed the PRA, including the Electronic Freedom of Information Act (EFOIA) Amendment of 1996.

The 1996 Electronic Freedom of Information Act amendment added a new level of clarity to the issue of electronic records. This amendment extended the right of citizens to access

executive agency records to include access to electronic formats and online information (Relyea, 2001). EFOIA also extended the time limit from 10 to 20 days to prohibit the use of agency backlogs as an excuse for noncompliance with information requests (Hammitt, 1999). The 1996 Clinger-Cohen Act further heightened the role of information technology in government. It established a CIO in every agency, making agencies responsible for developing an IT plan. Later, when e-government became a priority, the existence of the CIO strategic planning structure was an important element facilitating e-government implementation at the federal level.

Also in 1996, Congress passed the Personal Responsibility and Work Opportunity Reconciliation Act (PRWORA). This act, also known as the Welfare Reform Act, represented one of the first national pushes to incorporate the rhetoric of e-government with the routine services of agencies, specifically the administration of Temporary Aid to Needy Families (TANF). The act required interagency, interstate, and intergovernmental coordination of information-technology systems to ensure that no individual exceeded the allotted 5-year lifetime cap on assistance (Scavo & Shi, 2000). The failures associated with the PRWORA in terms of technology have been duly noted and offer a warning to e-government proponents about the harsh realities of creating interoperable, cross-platform systems.

In July 1996, President Clinton issued Executive Order 13011, which sought to improve the management of information technology at the federal level. It also provided broad support for coordinated approaches to technology application in the Executive Office (Relyea, 2001). Although this executive order mandated implementation of and adherence to the PRA and the Clinger-Cohen Act, it also focused on the alignment of technology goals with strategic organizational goals. The support for interagency coordination of technology is codified in Executive Order 13011. Mandated goal-alignment and technology-investment reviews are included in the directive as a method for reducing the failure rates and cost overruns associated with federal technology initiatives.

More recently, in 2001 the E-Government Act was offered for consideration in the U.S. Senate. This act, approved by the Senate in June 2002, mandated the establishment of an e-government administrator in the Office of Management and Budget, and also provided for considerable financial assistance to spur interagency e-government initiatives. Each of these legislative actions has strengthened the federal government's commitment to e-government.

One of the most significant information-technology developments at the federal level occurred after the tragedies of September 11th. The terrorist acts committed against the United States included the utilization of massive technology, notably the commercial aviation infrastructure, to perpetrate the crimes of mass destruction (Bonvillian & Sharp, 2001). The attack against America forced government officials to reexamine their information-technology policies, infrastructure, and systems. The newly established Office of Homeland Security and its associated directives comprise the largest centralization and consolidation effort involving governmental databases in the history of the United States. A recent General Accounting Office report (2002) highlights this effort and its challenges by examining the types of necessary data, the amount of data, and the transmission format of the data across vertical and horizontal governmental lines. The report also notes the challenges associated with traditional agency "stovepipes" and the need to move beyond this approach toward a centralized enterprise initiative (p. 8). The lack of connectivity and interoperability between

databases and agency technologies is another crucial challenge that must be overcome, it is argued, in order to create a comprehensive infrastructure to deal with issues of terrorism.

Another example of the critical need to centralize and consolidate government information in order to mitigate future terrorist attacks is found in the Chambliss-Harman Homeland Security Information Sharing Act (HR 4598). This act, passed by the U.S. House of Representatives in June 2002, mandates the dissemination of critical intelligence information from federal agencies, such as the Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI), to state and local governments (Dizard, 2002). The goal of this act is to further reduce the vertical stovepipes that exist between federal, state, and local governments with respect to information access and to encourage data sharing across all branches and levels of government in order to foster coordination and collaboration.

Another result of the September 11th attacks is the renewed concern about security issues related to information technology. These increased concerns have caused governments to reexamine the information they provide online and, in some cases, to restrict access to such information. Section 204 of the Homeland Security Act of 2002 allows the federal government to deny FOIA requests regarding information voluntarily provided by nonfederal parties to the Department of Homeland Security. Additionally, many government Web sites have removed potentially sensitive information. One example of the removal of sensitive governmental information involves the Department of Energy (DOE). According to the watchdog nonprofit organization OMB Watch, the DOE has removed detailed maps and descriptions of nuclear facilities with weapons-grade plutonium and uranium from its Web site (OMB Watch, 2002).

Although the effects of September 11th have impacted the use of information technology in the public sector in a variety of ways, there is little doubt that citizen demand for electronic information and services is likely to continue the trend of e-government adoption and expansion. According to the 2002 Pew Internet and American Life Project, Americans continue to use the Internet to access government information, research policy issues, contact elected officials, and participate in e-democracy in increasing numbers (Larson & Raine, 2002).

Theoretical Constructs

E-government has been viewed in a variety of ways. One context for examining e-government centers on recognition that e-government is more than just a shift in communication patterns or mediums. At least potentially, it involves a transformation of the organizational culture of the government. Recent authors argue that governments are mandated by citizen and business demands to operate within new structures and parameters precipitated by information technology (Bovens & Zouridis, 2002; Heeks, 1999; Ho, 2002; Osborne & Gaebler, 1992). Current demands require crosscutting services, which in turn require government to improve communication and interaction across traditional bureaucratic lines (Alexander & Grubbs, 1998). These new requirements, which fundamentally alter the nature of government, are made possible through the strategic use of information technology.

Garson (1999) has divided the theoretical frameworks of e-government into four main areas: decentralization and democratization, normative and dystopian, sociotechnical systems, and global integration theories. The first two suffice to explain basic variations in e-government

theory. The decentralization-democratization theory of e-government revolves around the progressive potential of technology and focuses on the positive governmental advances associated with e-government. Normative-dystopian theory emphasizes the high rate of conflict and failure associated with information-technology applications and counters the positivist progressivism of the decentralization-democratization theory with a realist view of inherent technological limits and contradictions. Each school of thought has its proponents as well as its critics. While neither framework can be considered fully descriptive, taken together they provide a useful delineation of the theoretical literature on e-government.

Decentralization-democratization theory is the most commonly held orientation associated with e-government. In fact, articles beginning with Bozeman and Bretschneider's seminal article in 1986 refer to the transformational, progressive nature of technology adoption in the government sector. Others have concluded that e-government and associated information-technology adoption lead to shifting paradigms, extending beyond the notion of simple progress (Ho, 2002; Reschenthaler & Thompson, 1996). Reschenthaler and Thompson are among theorists who note the revolutionary potential of information technology in government. They contend that the power of e-government technology lies in its ability to even the playing field for all sizes and types of governments. Additionally, they see in e-government the basis for reengineering the business of government, refocusing its work on the needs of the citizens and returning government to its core functions (Reschenthaler & Thompson). Other authors have also used the decentralization theory to highlight the transformational components of information technology and e-government.

Some authors examine the traditional bureaucratic model of public-service delivery (the Weberian model), which highlights specialization, departmentalization, and standardization (Ho, 2002; Weber, 1947). This traditional model has created the stovepipes associated with government—those departmental silos that resist functioning across agency boundaries. The main promise of the Weberian model is to ensure that all citizens are treated equitably with the utmost efficiency. However, in the 1990s, the reinventing-government movement sought to alter the core focus of government, moving from departmentalization and centralization to citizen-centric decentralization (Osborne & Gaebler, 1992), much in contrast to the Weberian model.

According to Ho (2002), the e-government paradigm, which emphasizes coordinated network building, external collaboration, and customer services, is slowly replacing the traditional bureaucratic paradigm and its focus on standardization, hierarchy, departmentalization, and operational cost efficiency. The new paradigm mirrors many of the tenets of the reinventing-government movement, including user control and customization, flexibility in service delivery, horizontal and vertical integration culminating in one-stop shopping, and innovative leadership focused on the end user (Ho; Osborne & Gaebler, 1992). This paradigm shift is precipitated by the advent of the Internet, which provides government the ability to use technology to impact customers directly instead of simply reengineering internal processes (Scavo & Shi, 1999).

A core concept of e-government, which falls under the decentralization orientation, is the idea of using technology as a linkage between citizens and government. According to the work of Milward and Snyder (1996), the governmental use of information technologies to engage and interact with the public further enhances the value of technology adoption, which in turn leads to greater e-government penetration. IT can be substituted for other

governmental institutions to link citizens to government services. This linkage causes both the citizens and the government to become reliant upon IT functions, increasing the penetration and adoption rates of e-government.

As governments—federal, state, and local—become more involved in information technology and gain recognition for their e-government efforts, other jurisdictions not currently engaged in e-government will increasingly become interested in and adept at this form of information-technology usage (Norris, 1999). That is, the decentralization theory predicts that e-government's diffusion will snowball as its benefits to citizens and to the agencies themselves is demonstrated.

Technology and e-government adoption rates are a key interest of decentralization proponents. In fact, the argument is virtually tautological: In order to define the factors that increase e-government penetration and adoption, one must believe in the positive potential of the concept. In terms of information-technology adoption and implementation, the greater the number of governments planning for and using information technologies and e-government approaches, the more legitimacy the technology gains (Fletcher, 1999). It is evident from the proliferation of e-government activities at the federal and state level that the widespread benefits of using information technology to provide more timely, seamless government services is a legitimate, even preferred, method of action. Citizen and business demands for e-government applications have extended to the local-government level and as more local governments begin using e-technologies, the legitimacy of the applications will further increases (Norris, Fletcher, & Holden, 2001).

By adopting new technologies, governments may be able to respond to the changing environment with improved service delivery, increased efficiency, and reduced costs (West, 2000). The use of e-government applications allows governments to more readily engage citizens and businesses in a virtual world that is thought to be more responsive and accountable to the needs of the customer. However, there is a marked lag in government adoption of new technologies and methodologies compared to implementation in the private sector.

The structural inertia that afflicts most governments, as well as risk aversion, means that governments are slow to adopt and implement new technologies. According to Herbert N. Casson, the government was one of the final sectors to adopt the telephone, approximately 10 to 15 years after its distribution to the public at large (Relyea, 2001). The lag associated with governmental adoption of new technologies continues today. In fact, research decades ago by Kraemer, Danziger, and King (1978) indicated that local government, in general, has had about a 10-year lag time between the introduction of a new technology and its adoption and use in localities. Furthermore, smaller local governments have a lag adoption time of 15 years or more. For government information-technology adoption and implementation, the inertia that exists within the public sector means that organizations are often less willing and able to engage new technologies (Bretschneider, 1990). The inherent tension between the need for reliability and accountability contrasted with reliance on maintaining organizational status quo leads to the increased adoption lag time in governmental organizations.

Support for e-government is allied with the decentralization theory, which offers optimistic prospects for the future of virtual governance. However, the stark reality of public technology and e-government failures has been repeatedly noted in news media. The concerns associated with privacy, security, and the digital divide are all common threads under normative-dystopian theory, which offers a critical approach to evaluating e-government. Proponents of

this view of e-government are traditionally concerned with the dehumanizing and isolating aspects of information technology. Recent concerns about the digital divide, the technology gap that exists between certain subpopulations in the United States, highlight the problems of fairly implementing technology as a mode of communication and service delivery. Fisher (1998) notes the disparity in power and access to technology that occurs in distinct subpopulations when analyzing grassroots social movements. His findings are consistently supported by other studies that note racial, regional, educational, gender, and age disparities among Internet users and technology owners (Norris, 2001; Novotny, 1998).

Bovens and Zouridis (2002) highlight the dystopian framework of e-government by examining the inherent problems associated with the application of information technology and the shift toward an e-government paradigm in real-world settings. They contend that the emerging emphasis on information technologies as the medium for citizen interaction with government fundamentally alters the role of the bureaucrat. The traditional Weberian model uses street-level bureaucrats to interact with citizens and to determine the proper services and service levels to assist these citizens (Lipsky, 1980). However, as technology becomes more integrated into government agencies, computer programs are often used to interface with clients, determine eligibilities, and decide upon proper levels of service (Boven & Zouridis). As a result of this new computer-based assessment trend, the street-level bureaucrats are losing their discretionary power. Bovens and Zouridis do not presuppose to judge the new, nondiscretionary technology models but rather use the paradigm shift to focus on the risks of arbitrariness and associated threats to the legitimacy of governmental actions at the street level.

Types of E-Government

Although several typologies have been developed to explain the progression of e-government (Layne & Lee, 2001; Moon, 2002), the UN and ASPA (2001) definition of the stages of e-government maintains continuity with the working definition set forth at the outset of this chapter. It is also important to note that the stages to be discussed do not represent a true linear progression, nor are they specific block steps. Rather, the stages are a continuum in which governments can be within the same stage with very different functionalities and service offerings.

According to the UN and ASPA (2001), there are five main stages of e-government. The lack of an organizational Web site is not defined by a stage, but may be considered Stage 0. Stage 1 is the emerging Web presence, which involves static information presented as a type of online brochure. The main goal of the emerging Web stage is to provide an online mechanism for communicating key general information about the government to interested citizens and entities. The Web site lacks information about services and is not organized in a citizen-focused manner. Typically, the government has used a "go it alone" approach, which visually represents the stovepipes or silos that exist within agencies—there is little coordination across agencies and levels of government in Stage 1 Web sites.

In Stage 2, enhanced Web presence, the role of the Web site becomes associated with information on services, although it is still organized by departments rather than by user groups. Enhanced Web presence sites typically have e-mail as a means of two-way communication. However, rarely are forms available for download. Stage 2 offers limited communication

and greater information about the services of the government, but it does not meet the citizen-centric approach that has been advocated for e-government.

Stage 3, interactive Web presence, begins to move into the citizen-centric realm of e-government. Typically, the information is portrayed by intuitive groupings that cross agency lines. For example, the Web site might use a portal as the single point of entry into various departments and service areas. The portal would offer major groupings like businesses, new residents, seniors, children, or other standard groups. Then, the end user would select the grouping that applies and be launched into a new section of the portal where the most common services requested for the group are located. The services would not be listed by departmental areas, but rather by functional areas. Stage 3 sites have downloadable forms with online submissions, e-mail contact for various governmental employees, and links to other governmental Web sites.

Stage 4, transactional Web presence, offers the ability to conduct secure online transactions. This stage is also organized by user needs and contains dynamic information. The Web site may offer a variety of transactions, including paying for services, paying bills, and paying taxes. Transactional Web presence includes the online submission of forms, many downloads, e-mail contact, and several links to other governments. The use of digital signatures also falls under Stage 4.

The final stage, Stage 5, involves seamless government. Although this stage represents an ideal, there is no real example of its application. Stage 5 involves a cross-agency, intergovernmental approach that only displays one front, regardless of service area. For example, a seamless Web site would offer local, state, and federal government services via the state

Table 1. E-government typology (Sources: Adapted from UN and ASPA, 2001; Ho, 2002)

Stages	Orientation	Services	Technology	Citizens
Stage 1: Emerging Web Presence	Administrative	Few, if any	Only Web	Going it alone
Stage 2: Enhanced Web Presence	Administrative, Information	Few forms, no transactions	Web, e-mail	Links to local agencies
Stage 3: Interactive Web Presence	Information, Users, Administrative	Number of forms, online submissions	Web, e-mail, portal	Some links to state and federal sites
Stage 4: Transactional Web Presence	Information, Users	Many forms and transactions	Web, e-mail, digital signatures, PKI (public-key infrastructure), portals, SSL	Some links to state and federal sites
Stage 5: Seamless Web Presence	Users	Mirror all services provided in person, by mail, and by telephone	Web, e-mail, PKI, digital signatures, portal, SSL, other available technologies	Crosses departments and layers of government

portal without the end user recognizing what level of government provides the service. A Stage 5 site would offer vertical and horizontal integration and would require true organizational transformation with respect to administrative boundaries.

With a working knowledge of the typology associated with e-government, it is easy to assess the current status of the concept. Much of the literature indicates that Stage 2, enhanced Web presence, is the typical placement of an American local government on the e-government continuum. Alexander and Grubbs (1998) note, "Few sites capitalized on the interactive nature of the Internet to conduct public discussions, maintain bulletin boards, or provide data and information available for download." However, local governments are making strides in this arena, spurred by the recognition of the Web site as a vital economic development tool.

A review of the 2004 International City and County Managers Association's e-government survey finds that approximately 90% of cities and counties with populations over 2,500 are not offering transactional Web sites. Furthermore, based on the 2004 ICMA e-government survey, only 8.6% of cities and counties offer the online payment of taxes, 9.2% offer the online payment of utility bills, and 7.3% offer the online payment of fines and fees. The state and federal government offer more robust transactional services, but local governments are recognizing the need to offer electronic services to satisfy customers as well as to reduce the costs associated with traditional walk-in and mail service delivery. E-government will continue to be a critical area for local-government investment as citizens, businesses, employees, and visitors increasingly expect Internet-based options for governmental services.

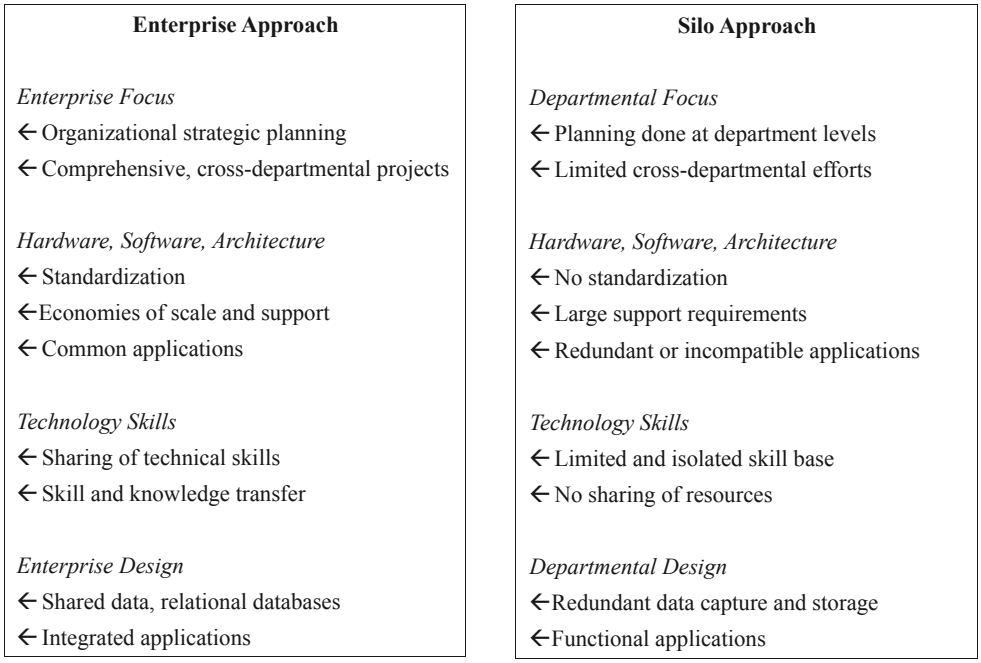
E-government has been viewed in a variety of ways. One context for examining e-government centers on the recognition that e-government is more than just a shift in communication patterns or mediums. At least potentially, it involves a transformation of the organizational culture of the government. Recent authors argue that governments are mandated by citizen and business demands to operate within new structures and parameters precipitated by information technology. These new requirements, which fundamentally alter the nature of government, are made possible through the strategic use of information technology to accomplish enterprise goals.

Enterprise Approaches

The primary management goal for information technology is to support the business objectives of the local government and to facilitate departmental efforts to provide efficient and effective services to the citizens, businesses, and visitors. Information technology has become a strategic partner in the governmental efforts to provide high-quality, consistent, and equitable services. The driving vision for information technology within many governments includes the development of an enterprise-wide focus on IT, a focus on the customer, and the use of IT as an enabler in efficient and effective customer service. This vision marks a significant departure from the traditional government silo approach with its individualistic, department, or agency-centric efforts, as illustrated in the following chart.

Many future technology efforts will cross multiple local government departments with a single goal of providing services to the citizens, businesses, and visitors. In this new environment, technology is used as the basis for communication, interoperability, and data and

Figure 1. The changing landscape of technology-enabled government



resource sharing. Furthermore, technology is the vehicle through which cost reduction can occur by increasing efficiency and effectiveness of services through the use of an enterprise architecture and standards. State and local governments throughout the nation are using enterprise approaches to achieve high levels of return on investments, greater customer satisfaction, and increased cost savings.

Chief Information Officers and Professional Staffing

Information technology has fundamentally altered many aspects of daily life, including interactions with public and private sectors. The role of the Internet continues to increase as more citizens use it to find pertinent information, purchase goods and services, and participate in virtual communities. By capitalizing on the Internet revolution, governments can create new channels of communication and new methods for participation via e-government. The changing environment, coupled with citizen and business demands, encourages government involvement in e-government initiatives and related uses of information technologies.

CIOs emerged as a mechanism to connect the business units in an organization with the information-technology staff. In essence, CIOs are the linchpins between these two seemingly disparate, and often contentious, components of an organization. In the past few decades, CIOs have been revered as supreme organizational aligners and lamented as overtitled technocrats. Regardless of the hype and hyperbole surrounding the role of chief information

officer, one thing is certain: The job of CIO is always demanding and often difficult. The CIO is responsible for disseminating the critical technology plans to senior executives in order to engender their support while maintaining one foot firmly entrenched in the realm of new and emerging technologies. The CIO must possess the vision for the future while maintaining an eye on the historical legacies of the organization. Too often, chief information officers are forced to take sides between the business units and the information-technology department when, in fact, their role is to build the bridges between these organizational silos. The role of the CIO is critical and the job requires skillful navigation of the various minefields and bear traps that can ensnare and destroy technology projects.

As established as the role of CIO is within the private sector, it is only just emerging in the public sector. The role of the CIO has been adopted from the private sector as one way to navigate the emerging reality of public-sector information technology and e-government. As early as 1981, the title of CIO emerged in the private-sector literature as the defined leadership role for information technology. Extensive research has been conducted on the attributes and characteristics of successful CIOs in the private sector. Some of the most commonly cited traits include being a generalist, having significant power and authority in the organization, and providing a common vision for the implementation of strategic information technology. Based on the success of the CIO in providing leadership and status to information-technology projects in the private sector, the federal public sector followed suit by institutionalizing the position with the passage of the 1996 Clinger-Cohen Act.

The 1996 Clinger-Cohen Act heightened the status of information technology in government. It established a chief information officer in every federal agency, making agencies responsible for developing an IT plan. Now as e-government becomes a priority at the federal, state, and local government levels, the existence of the CIO and a strategic planning structure becomes critical to facilitating e-government implementation. The importance of successful IT projects and their requisite investments is critical in both public and private sectors, as evidenced by the Clinger-Cohen Act and solidified by the rapid proliferation of CIOs in a variety of public and private organizations.

Conclusion

Information technology has fundamentally altered the way we interact in today's society. The role of the Internet continues to increase in society as connectivity becomes more readily available to disparate geographical and demographic sectors of the United States. E-government offers an opportunity to create new channels of communication and new methods for participation. The success of existing e-government efforts provides increased legitimacy for further information-technology adoption (Norris, 1999). The changing information environment and the movement toward the knowledge economy, juxtaposed against citizen and business demands, mandate that government become involved in e-government initiatives and related uses of information technologies (Ho, 2002).

It is clear that the advent of technology has fundamentally altered the way governments conduct business. States, cities, and counties are using technology to improve service delivery, enhance efficiency, and increase transparency and accountability. The citizen and business

demand for electronic access to building permits, dog licenses, and birth certificates has heightened the need for investing in information technology. Even more importantly, many governments are moving away from traditional bureaucratic emphasis on departmental silos and information isolation to a new paradigm that emphasizes coordinated network building, external collaboration, and customer services due to information-technology investments. Furthermore, information technology is providing new opportunities for civic engagement and participation from a variety of citizens and groups. The public sector has been engaged in the information-technology revolution and the continued investment and support of these efforts is imperative.

References

Alexander, J. H., & Grubbs, J. W. (1998). Wired government: Information technology, external public organizations, and cyberdemocracy. *Public Administration and Management: An Interactive Journal, 3*(1). Retrieved from http://www.pamij.com/

Bonvillian, W. B., & Sharp, K. V. (2001). Homeland security technology. *Issues in Science and Technology*, 43-49.

Bourdourides, M. A. (2001, October). *New ICTs policies.* Paper presented at ICITA 2001 Conference, Berlin, Germany. Retrieved from http://www.math.upartas.gr/~mboudour/

Bretschneider, S. (1990). Management information systems in public and private organizations: An empirical test. *Public Administration Review, 50*(5), 536-545.

Dizard, W. (2002). House oks data-sharing bill. *Government Computer News, 21*(17). Retrieved from http://www.gcn.com/21_17/news/19182-1.html

Fisher, D. (1998). Rumoring theory and the Internet: A framework for analyzing the grass roots. *Social Science Computer Review, 16*(2), 158-168.

Fletcher, P. D. (1999). Strategic planning for information technology management in state governments. In G. D. Garson (Ed.), *Information technology and computer applications in public administration: Issues and trends* (pp. 81-97). Hershey, PA: Idea Group Publishing.

Fountain, J. (2001). *Building the virtual state: Information technology and institutional change.* Washington, DC: Brookings Institution.

Garson, G. D. (1999). Information systems, politics, and government: Leading theoretical perspectives. In G. D. Garson (Ed.), *Handbook of public information systems* (pp. 591-605). New York: Marcel Dekker, Inc.

General Accounting Office. (2002). *National preparedness: Integrating new and existing technology and information sharing into an effective homeland security strategy* (GAO-02-811IT). Washington, DC: Government Printing Office.

Gore, A. (1993). *Creating a government that works better and costs less: Reengineering through information technology* (Report of the National Performance Review). Washington, DC: Government Printing Office.

Hammitt, H. (1999). The Legislative Foundation of Information Access Policy. In G. D. Garson (Ed.), *Handbook of public information systems* (pp. 27-40). New York: Marcel Dekker, Inc.

Heeks, R. (1999). Reinventing government in the information age. In R. Heeks (Ed.), *Reinventing government in the information age* (pp. 9-21). New York: Routledge.

Ho, A. T.-K. (2001). Reinventing local government and the e-government initiative. *Public Administration Review, 62*(4), 434-444.

Horrigan, J. B. (2003). Consumption of information goods and services in the United States. *Pew Internet and American Life Project.*

Kettl, D. (2000, June). *The transformation of governance: Globalization, devolution, and the role of government.* Paper presented at the Spring Meeting of the National Academy of Public Administration. Retrieved from http://www.lafollette.wisc.edu/research/publications/transformation.html

Kim, P. S. L. W., & Wolff. (1994). Improving government performance: Public management reform and the National Performance Review. *Public Productivity & Management Review, 18*(1), 73-87.

Kraemer, K. L., Danziger, & King. (1978). Local government and information technology in the United States. In *Local government and information technology.* Paris: OECD Informatics Studies #12.

Landsbergen, D., Jr., & Wolken, G., Jr. (2001). Realizing the promise: Government information systems and the fourth generation of information technology. *Public Administration Review, 61*(2), 206-220.

Larsen, E., & Raine, L. (2002). The rise of the e-citizen: How people use government agencies' Web sites. *Pew Internet and American Life Project.* Retrieved from http://www.pewinternet.org/reports/pdfs/PIP_Govt_Website_Rpt.pdf

Layne, K., & Lee, J. (2001). Developing fully functional e-government: A four stage model. *Government Information Quarterly, 18*(2), 122-136.

Milward, H. B., & Synder, L. O. (1996). Electronic government: Linking citizens to public organizations through technology. *Journal of Public Administration Research and Theory, 6*(2), 261-276.

Moon, M. J. (2002). The evolution of e-government among municipalities: Rhetoric or reality? *Public Administration Review, 62*(4), 424-433.

Moulder, E. (2001). E-government … If you build it, will they come? *Public Management, 83*(8), 10-14.

Norris, D., & Kraemer, K. (1996). Mainframe and PC computing in American cities: Myths and realities. *Public Administration Review, 56*(6), 568-576.

Norris, D. F. (1999). Leading edge information technologies and their adoption: Lessons from US cities. In G. D. Garson (Ed.), *Information technology and computer applications in public administration: Issues and trends* (pp. 137-156). Hershey, PA: Idea Group Publishing.

Norris, D. F., Fletcher, P. D., & Holden, S. H. (2001). *Is your local government plugged in? Highlights of the 2000 Electronic Government Survey.* Paper prepared for the International City and County Managers Association and Public Technologies, Incorporated. Retrieved from http://icma.org/download/catIS/grp120/cgp224/E-Gov2000.pdf

Norris, P. (2001). *Digital divide: Civic engagement, information poverty, and the Internet worldwide.* Cambridge: Cambridge University Press.

Novotny, P. (1998). The World Wide Web and multimedia in the 1996 presidential election. *Social Science Computer Review, 16*(2), 169-184.

OMB Watch. (2002). *Access to government information post-September 11th.* Retrieved August 24, 2002, from http://www.ombwatch.org/article/articleview/213/1/104/

Osborne, D., & Gaebler, T. (1992). *Reinventing government: How entrepreneurial spirit is transforming the public sector.* Reading, MA: Addison-Wesley.

Rahm, D. (1999). The role of information technology in building public administration theory. *Knowledge, Technology, and Policy, 12*(1), 74-83.

Relyea, H. C. (2001). E-gov: The federal overview. *The Journal of Academic Librarianship, 27*(2), 131-148.

Reschenthaler, G. B., & Thompson, F. (1996). The information revolution and the new public management. *Public Administration Research Theory, 6*(1), 125-143.

Rocheleau, B. (1999). The political dimensions of information systems in public administration. In G. D. Garson (Ed.), *Information technology and computer applications in public administration: Issues and trends* (pp. 23-40). Hershey, PA: Idea Group Publishing.

Scavo, C., & Shi, Y. (1999). World Wide Web site design and use in public management. In G. D. Garson (Ed.), *Information technology and computer applications in public administration: Issues and trends* (pp. 246-266). Hershey, PA: Idea Group Publishing.

Scavo, C., & Shi, Y. (2000). The role of information technology in the reinventing government paradigm: Normative predicates and practical challenges. *Social Science Computer Review, 18*(2), 166-178.

Seneviratne, S. J. (1999). Information technology and organizational change in the public sector. In G. D. Garson (Ed.), *Information technology and computer applications in public administration: Issues and trends* (pp. 41-60). Hershey, PA: Idea Group Publishing.

Sprecher, M. H. (2000). Racing to e-government: Using the Internet for citizen service delivery. *Government Finance Review, 16*(5), 21-22.

United Nations (UN) & American Society for Public Administration (ASPA). (2001). *Benchmarking e-government: A global perspective. Assessing the UN member states.* Retrieved from http://www.unpan.org/egovernment2.asp

West, D. M. (2000). *Assessing e-government: The Internet, democracy, and service delivery by state and federal government.* Taubman Center for Public Policy at Brown University. Retrieved from http://www.brown.edu/Departments/Taubman_Center/polreports/egovtreport00.html

Chapter VII

E-Participation Models

Suzanne Beaumaster, University of La Verne, USA

Abstract

Participation is the cornerstone of our governance process and has manifested in a variety of constructs since the inception of our government. As public agencies and political leaders discover the possibilities offered by technological mediums, the question becomes, what kind of participation should we be fostering and what do we hope to gain through participative processes? The opportunities to enhance our understanding and approach to democracy have grown tremendously in the past decade. Through technological means, more individuals can gain access to public dialogue and discourse. Given the nature of recent technological opportunities, public leaders are considering the possibilities of e-governance and within that framework, e-participation. This chapter provides a definition and discussion of three e-participation models: information exchange, general discourse, and deliberation. In addition, the chapter will address the issues, characterizations, and criteria that are closely related to the development of electronic participation in the governance process.

Introduction

The advent of the information age has brought with it a host of new monikers for our public-administration lexicon. These terms—e-democracy, e-government, and e-participation—express the direction we are heading with regard to government processes and citizen access. Today no discussion of issues surrounding government or administration can exclude concerns of our new, virtual world, where we engage in business dealings, administration, personal activities, discourse, and government electronically. The issues we have concerning all of these matters must now be discussed with an eye for the implications of what it means to engage virtually. Virtual communities are developing around us, outside of physical space; as these virtual spaces evolve and take shape, individuals, institutions, and governments must reframe their perspectives to meet challenges posed by emerging interactive environments. Old challenges malinger while entirely new challenges must be addressed outside of our conventional perspectives. E-government, and within it e-participation, is one such issue.

The Participation and E-Participation Relationship

E-participation is an approach, a technique, and a tool simultaneously, representing a new way of addressing old problems or issues, specifically regarding citizen access to government processes. In addition, e-participation structures a particular set of activities through which the public can gain information and services, and deliver input. Finally, e-participation is a specific tool for the development and enhancement of public participation as well as a means for access to elected officials and administrators. In other words, e-participation is not just a new way of doing the same old thing, but has the potential to transform citizen access.

Our current participatory structure has grown out of the problematic nature of representative democracy. Since the inception of our government, an ongoing discussion persists regarding the desirability and practicality of direct citizen participation in public decision making (Abilock, 2005; Morse, 2006; Noam, 2005; Timney, 1998). Given the representative nature of democracy in the United States, matters of equity and access are at the forefront of any discussion regarding citizen access and input into the governance process whether done so electronically or via more traditional systems.

In an ideal sense, citizen participation is a hallmark of the democratic process in the United States. However, in reality the transaction costs to obtain information and impart influence are borne differentially by citizens. The desire to interact as a significant member of the governance process necessitates being knowledgeable on the issues to a degree that has proven difficult to achieve for a variety of reasons. Government decision making is comprised of a complex network of political officials, technical experts, interest groups, organizations, administrators, and citizens. Effective input in these decisions demands some degree of sophistication in navigating the complex features of a given issue or problem. With increasing institutional interdependence comes increasing complexity, posing challenges for access and influence that even the well-heeled citizen may find daunting. Regardless of the intricacies involved, it is the citizen who must acquire the status of being informed in order to achieve legitimacy within the system. As the information age brings about new

opportunities for participation, governance must address some significant issues including the following. How important is citizen interaction for effective decision making? What level of input is appropriate? To what degree should government facilitate the process of informing the citizenry?

Dealing with the Questions of Participation

There is a great deal of consensus in the literature to support the argument that citizen participation is not only a hallmark of our governance process, but fundamentally necessary for effective decision making. The spirit of this perspective finds its roots in the belief that citizens are interested in public decisions and the issues facing our society; furthermore, it is one of the duties of government to ensure that the citizens are provided the information necessary to be substantively part of the governance process. In the words of Thomas Jefferson,

I know of no safe depository of the ultimate powers of the society but the people themselves, and if we think them not enlightened enough to exercise their control with a wholesome discretion, the remedy is not to take it from them, but to inform their discretion. (as cited in Dumbauld, 1955, p. 93)

From this perspective, in any medium, electronic or traditional, citizen participation is a primary goal. There is a great number of arguments to support the position that participation is fundamental to our governance process. Kathi and Cooper (2005) posit that participation may be viewed either morally or instrumentally. The former suggests that it is a citizen's right in a democratic society to participate in the process of government. The latter perspective provides that participation, at the very least, is necessary for stability within the political community. In addition, the instrumental participation promotes efficiency and effectiveness as well as laying the groundwork for social change. While democracy by its very nature demands the participation of its citizens, practical application of the ideal is much more problematic, especially given the institutional stature conferred on public representatives at all levels of government.

Participation and the Democratic Process

Fundamentally, involvement in decision making by the public improves the democratic process through the enhancement of the regulatory process. In essence, it supports the individual's right to be heard and to influence government activities (Holman & McGregor, 2001). In many ways, public participation is as much about the democratic process as it is about outcomes. There is something to be said for being involved regardless of whether or not your input becomes part of the ultimate decision, policy, or agency plan. As stated by Charles White (1997, p. 24), "Democratic theory envisions a system of government organized as much to foster deliberation as to guarantee participation." In this way, citizens take

ownership of the process as well as the outcomes. In essence, the activity of participation sets in motion a chain of events as it were. If people participate in public decision making, then the decisions have a greater likelihood of reflecting what is of concern to the specific community. It follows that higher levels of individual participation lead to a greater feeling of ownership in the process, which may lead to an increased level of interest for other future civic activities. Finally, the greater the level of overall participation, the harder it is for public officials to ignore the concerns, ideas, and input of the citizenry (Al-Kodmany, 2000).

Of course there has always been some dispute with regard to the desirability and viability of public participation. The dissenting opinion fears that too much democracy is as problematic as too little. This has been of concern since the very outset of our constitutional beginnings; a prominent example is found in Federalist 10 where Madison speaks to the fears surrounding the judgment of the general public. His argument states,

to refine and enlarge the public views, by passing them through the medium of a chosen body of citizens, whose wisdom may best discern the true interest of their country, and whose patriotism and love of justice, will be least likely to sacrifice it to temporary or partial considerations. (Cooke, 1982, p. 62)

The opposition to more participation has always maintained that an informed or elite citizenry are more suitable for the task of public decision making than the general, often uninformed public. This perspective argues that direct participation is not an especially effective or efficient way to inform decisions (Innes & Booher, 2004). This viewpoint claims that the methods of public participation, which are legally required, do not achieve that which they are formally bound to accomplish—that is, to review, comment, and provide input on public decisions. Typically, participants in this process are quickly disillusioned; citizens and public officials alike find themselves in an untenable situation. Citizens feel disenfranchised and administrators are beset with all manner of input, which they often find erroneous, cumbersome, and irrelevant. The supporters of this argument speak to the question of what is required to really achieve actual participation in the governance process. The general feeling on the issue suggests that the current system does not satisfy public participants' desire to truly be part of the working dialogue involved in shaping decisions. The worst-case scenario is that current practices actually polarize and antagonize those who are attempting to engage and contribute to the process (Innes & Booher).

As Kathi and Cooper (2005) describe, the commitment to citizen participation is conflicted. On the one hand, such civic engagement is encouraged based on our traditional approach to democracy, yet the framework of the system is designed to "protect political and administrative processes from an active citizenry" (p. 560). Essentially, the technical elite maintain control over decisions within the public sphere and the lack of responsiveness to citizens continues to plague the process.

As the discussion over the best practices for democracy continues, it appears that we are achieving somewhat of a middle ground. The prevailing perspective supports indirect forms of participation such as voting while at the same time acquiescing to the fact that some more direct methods of public participation are needed. This certainly leaves us with agreement that citizen participation should be supported as a fundamental component for decision making. Unfortunately, this agreement is often only grudgingly supported or paid lip service to as a

necessary evil. In the 1990s, the "reinventing government" movement (Osborne & Gaebler, 1992) brought this discussion into bold relief. The businesslike approach to government advocated by the reinventing trend canonized a passive customer or user of services over and above an active citizen or direct participant in governance (Innes & Booher, 2004). At best, we are left with some sense of ambivalence about public participation; in the worst case, it may be completely ignored as a part of the governance process. Given the apparent discord surrounding the general issue of citizen participation, it would seem that any further discussion of adding a new ingredient to the mix might muddy the issue even further. What is not in doubt is the fact that government in general and participation constitutively are now moving in the direction of electronic formats. Questions remain as to what role e-participation should assume. Is e-participation more functional as a supplement to the traditional format or should it serve as a replacement for the existing system? What are the overarching purposes of e-participation?

Purposes of E-Participation

Given the problematic reality of participation in general, it would seem that the viability of participating in an electronic format would fare no better. Certainly citizen apathy is not just a result of inconvenience. Thankfully, e-participation is not just a tool that makes access to the government process more convenient. There are a host of purposes that e-participation serves. Following are some of the current objectives that may be fulfilled.

- Participating electronically is convenient. The Internet as a medium offers 24/7 access and there is no need to go to the location of the service in order to acquire information, access services, or conduct business. The anytime and continuous format that e-participation allows can foster more thoughtful engagement over and above the immediate-response format demanded of most real-time venues.
- E-participation allows access to a broader audience (Macintosh, 2004). The range is extensive and essentially borderless.
- The digital format and the use of the Internet allow for many different communication mediums. Participation is supported using multiple technologies that can mitigate numerous circumstances: language barriers, audio and visual deficiencies, transportation issues, individual skill levels and educational differences, communication differences, and technological capacity (Carver, Evans, Kingston, & Turton, 2000).
- Individuals who are unable or unwilling to engage in discourse face to face have access to a medium that allows them to engage at their own pace, over time, with an opportunity to review and revise. This may serve to reduce anxiety and produce more active participation. In addition, e-participation allows for individualized (personal) expression.
- E-participation is informative from multiple perspectives. It provides policy and decision makers with a perspective on public preferences as well as enhancing decisions through the incorporation of the public's knowledge base. From a second perspec-

tive, e-participation can "provide relevant information in a format that is both more accessible and more understandable to the target audience to enable more informed contributions" (Macintosh, 2004, p. 2). Information can be tailored for multiple levels of understanding. An individual reviewing an issue can "drill down" through increasing levels of complexity. In this way, complex relationships can be presented in a user-friendlier format. A user might explore the data and explanations of a given issue through multiple levels of hyperlinks and subsequently engage in dialogue more informed and better prepared.

- E-participation has the capacity to draw in a broader audience and through various methods, promote deeper, more deliberative participation (Macintosh, 2004).
- Finally, through the use of a variety of information technologies, e-participation allows public officials to archive information as well as citizen input on any given issue. In this way, the electronic medium supports case building and the tracking of trends.

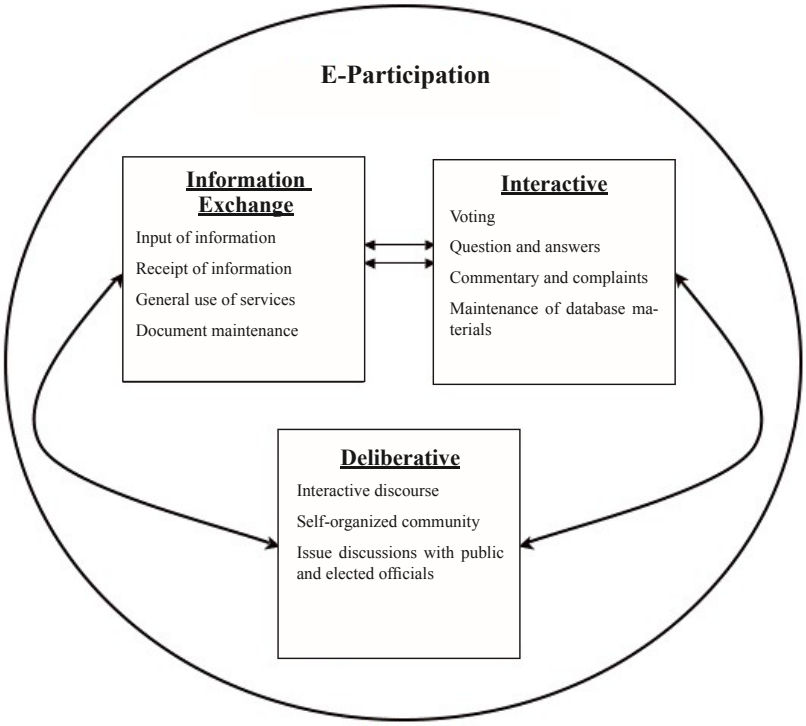
E-participation is one of the ways in which democracy is being reshaped. The increase in digital information as well as communication technologies opens up a multitude of possibilities for enhancing public-service delivery, discourse, and citizen-involved decision making. The key is to determine how e-governments should operate and what the nexus is of their functionality. It is also important to ascertain both the desirability and feasibility of e-participation with specific concerns for realistic returns on the initial investments. Specific to this discussion is the question of how e-participation should be addressed by those responsible for creating the commitments and armature that e-participation requires.

E-Participation Models

In its current state, e-participation can be broken down into three types, which are not mutually exclusive. They are information exchange, interactive services, and deliberative participation. Figure 1 shows a three-zone model representing these types and their relationships. Each component of the model functions in conjunction with the others.

The exchange of information as one-way communication and interactive participation as a two-way interchange function closely together. Individuals who access a government Web site typically begin the process because they are looking for specific information; this level of engagement constitutes participation as information exchange. The users then find themselves accessing particular government services or engaging in indirect participatory behavior such as voting, paying utility bills, or reviewing commentary. This commitment level provides a base from which the evolution of e-participation can begin. Accessing a city Web site in order to find information about area parks and recreational services may lead to reserving the park and paying associated fees using an online form. The progressive nature of e-participation can further evolve as the public continues to make use of online information and services; they become more interested in issues regarding specific services and the municipality at large. This is where the process leads to e-participation at the deliberative level. Deliberative e-participation reflects a more interactive version of the citizens interfac-

Figure 1.



ing with government. This fully engaged zone of participation encompasses direct forms of participation representing two-way, interactive discourse between citizens and citizens, and between citizens and public officials. Such dialogue becomes a stepping-stone for the ongoing development of public interest in online communities.

Information Exchange

As mentioned above, the model of e-participation presented here encompasses a range of participatory approaches. At one end of the spectrum is information exchange. This portion of the model incorporates what is often described as the general delivery of public information. Although certainly not an exhaustive list, the following are included: municipality or agency data, community information, frequently asked questions (FAQs), contacts, available services, and even information about private-sector services related to the given organization. Almost all government agencies and municipalities have some kind of informational Web site. These range from the simple to the sublime. The greater majority of public institutions have designed their electronic portals to include a full range of government services, including everything from information about upcoming events and paying traffic tickets to reviewing building permits as well as transcripts of council sessions.

Developing a framework for e-participation necessitates a discussion of where participation actually starts; as is the case with so many other aspects of life, half the battle is just showing up. What does this mean electronically? When a citizen accesses information or public services in an online format, is that participation? A good argument can be made that information exchange is the place where e-participation truly begins (Hudson-Smith, Evans, & Batty, 2005)—the first step toward the evolution of an informed public. While this kind of basic information does not necessarily constitute a deeply informed populous, it is a start. The convention of providing access to public information or delivering services online is in many ways a factor of convenience. At this level of e-participation, the public is engaging in a unidirectional relationship with government as the producer and citizens as the consumers (Macintosh, 2004). In this way, information exchange is a medium for citizen involvement at its most base level. In essence, bringing the public to a government Web site is a more convenient and efficient way for many citizens to conduct business on a day-to-day basis. Over the last 10 years, most generalized government services have moved to the Web and are now accessible in electronic format. The functionality of the governance process is enhanced by convenience, accessibility, and availability 24/7. Through this medium, citizens have become accustomed to the electronic format; moreover, the more people use online systems, the more comfortable they become, thus paving the way for further electronic interactions.

Information Exchange as Participation

Information exchange constitutes the most fundamental of functional activities with regard to governance, and while it represents the most minimal form of civic engagement, it is, after all, participation. One of the fundamental components of democratic theory is the principal of political equality, which supports the equal opportunity for each citizen to influence political activity and public decision making should they choose to do so (Rosenbaum, 1978). The key component here is choice. In this sense, the individual citizen's choice to access information electronically represents the occurrence of participation. The facilitation of public participation through the delivery of information further supports the participative process. In this day and age, the electronic posting of municipal information is a given: In this way, e-government assumes at least this level of participation no matter how minimal it may appear in the grand scheme of things.

Even at this most basic level, individual ownership of the process can take shape. A sense that an exchange is possible—along with the discovery that not only is information readily available but that access is relatively easy—can open the door for increased demand of both information and services. Information exchange is a critical part of the e-participation model primarily because it lays the foundation for the effectiveness of both the interactive and deliberative components. Holman and McGregor (2001) describe three factors directly related to the effectiveness of e-participation: "information and information flow, level of preparedness, and timeliness" (p. 165). The authors argue that public participation increases the demand for information and that the knowledge gained in turn prompts further, more informed participation. This, it would seem, is a self-perpetuating cycle. This process has the added benefit of raising the level of confidence that public officials have in citizen input. At the information-exchange level, information is typically "process information"

(Holman & McGregor), which is one-way communication from government to the citizen. The accessibility of process information in a timely manner provides two of the necessary components for the preparation of the public as an informed citizenry. Whether it is citizens or, instead, public agencies who drive the need to obtain information, the fact remains that it is a critical resource in the decision-making process.

Interactive E-Participation

The second component to the model presented here is interactive e-participation. On the one hand, citizen interaction is fairly functionalist, providing day-to-day access and usage of government services, electronic correspondence with public officials, or information review and commentary. This particular element is characterized by a two-way relationship. Macintosh (2004) refers to this type of participation as "consultation" in which "citizens provide feedback to government" (p. 2). In this case, it is the agency or public officials who define the parameters of the discussion while citizens provide input and opinions as needed or requested.

Delivering services virtually is at the core of any organizational presence online. The idea began its development in the 1980s as businesses and municipalities considered the possibilities of creating the virtual delivery of services; at the outset, this was primarily entertainment options and online shopping (Hudson-Smith et al., 2005). As information technology evolved, becoming more prevalent and user friendly, the medium became a central part of the design of e-government (Hampton, 2003).

At this level of interaction, participation starts when a citizen chooses to access a service electronically. While this may not seem to have the magnitude necessary to represent true e-participation, it does provide a gateway to civic opportunities. Participation at this level means that the necessary groundwork has been laid technologically to promote further aspects of e-government. In addition, it indicates a desire by the public to make use of electronic or technologically based approaches to conventional activities. It has been argued that technologies can "stimulate participation in democratic processes," which enhances an individual's sense of civic belonging (Hudson-Smith et al., 2005, p. 68). In addition to allowing greater access, ease of use, and convenience, online interaction provides an antecedent to creating a sense of involvement in a virtual community. A strong foundation for continued citizen engagement may be fostered through the facilitation of an online community at this level. After all, no participation happens over night; it is a developmental process.

Deliberative E-Participation

While both information exchange and interactive e-participation are important components for a fully functioning participation model, more direct participation is necessary in order to truly achieve effective governance. The element that brings this model together is de-

liberative e-participation. This particular component is characterized by advanced levels of communication, which go beyond two-way interactions. The argument here is for the development of collaborative discourse between government and citizens. This arrangement calls for active public engagement in all aspects of decision making, entailing public involvement in the complete process including defining the issues and problems, general commentary and input toward the knowledge base, and finally agenda setting and evaluation. Similar conceptualizations have referred to this level of e-participation as "active participation" (Macintosh, 2004, p. 2), "e-regulation" (Garson, 2006, p. 83), and, from a traditional perspective, "active," "transition" (Timney, 1998, pp. 93-94), and "deliberative democracy" (Weeks, 2000, p. 360).

An excellent framework is presented by Mary Timney (1998), which raises questions for the development of e-participation design. The two possibilities she presents that have applicability for this discussion are (a) government with the people or (b) government by the people. On the first account, Timney describes a "hybrid or transition" form of participation in which citizens share control with decision makers. The problem definitions are developed by the agency, but the ensuing process is open, promoting the desired outcome of consensus. In this case, the public administrators both participate and facilitate. In the second case or "active" model, the author describes a scenario in which the citizens are in control of the entire process. In this case, the agency and administrators act as functional support and consultants. This is government by the people and represents full ownership by citizens—the extreme end of the direct participation spectrum. Certainly, either of these approaches can be achieved in electronic participation formats, with technology allowing for the development of either scenario. The question becomes, given the nature of representative democracy and participation in general, which framework offers the greatest possibility of achieving effective e-participation?

Conceptualizing Deliberative Participation

This conceptualization of e-participation necessitates a set of criteria that is the benchmark of public deliberation. First, citizens must be provided balanced, accessible, and credible information. Deliberation requires that an individual be reasonably informed on the particulars of the issue. While the provision of information does not mean that each individual will make use of it in the same way, or even at all, efforts must still be made to supply adequate information. As discussed with regard to information exchange, the use of technologies allow for a variety of possibilities. Data can be tailored for individual needs, circumstances, and expertise levels. A broader range of services can be offered electronically to more locations and to accommodate a variety of circumstances.

Second, citizens must be allotted adequate time in which to deliberate. The majority of public issues are not simple by any stretch of the imagination. Even with the best information and adequate understanding, the average citizen will need the time to think through the issue. An additional concern in this regard is the openness of the parameters by which each citizen is asked to deliberate. This level of public participation necessitates much greater degrees of depth and tends to be much broader in scope. The discussion must be open to expansion and revision as individuals engage. One of the most ideal characteristics of electronic delivery methods is their transcendence of time and geography. Information and opportunities for

engagement may be made available 24/7 and to the farthest reaches of a community.

It is easy to imagine that open and expansive dialogue might be in danger of devolving into something of a free-for-all, especially considering the relative anonymity and accessibility of the electronic medium. Given this possibility, a third criterion is in order: that of a regulated format. As in any discussion, rules of conduct must be set in order to maintain a viable atmosphere for dialogue. The electronic format allows for rules to be agreed upon and set, as in any other environment. However, technology allows for much stricter maintenance of these rules. Time frames can be easily upheld; discussions may be shut down at the end of the allotted period. Users in violation of protocol can be blocked. A wide variety of solutions may be employed to maintain the viability of online discussions.

Finally, deliberative participation requires that the sample of citizens be inclusive, interactive, and representative of the broader population. In any participation model, this means that efforts must be made to include participants who represent those concerned with or affected by the issue at hand. In an electronic format, this typically means addressing the digital divide. Online access must be available for those who typically do not have equal representation as well as those who are less literate or apprehensive of technology, and individuals who are socially marginalized. Information technologies make it possible for more and more citizens to become involved in public discourse. Access points can be made available at a variety of public locations and training modules can be built into most systems. With the rapid advancement of technology come more and more options for delivery and increased user friendliness. In addition, the electronic medium helps strip away many designations that have tended to increase the likelihood of status-based bias or influence. Certainly, the differences between citizens are less obvious, especially typical identifiers such as race, gender, and wealth.

Criteria for Deliberative E-Participation

It is when e-participation becomes deliberative that it can begin to meet the criteria of real effectiveness. While measures of effectiveness can be difficult to come by, Innes and Booher (2004) provide a very usable set of criteria for participatory effectiveness: "supports interaction, dialogue, and collaboration; inclusive; defines future actions; self-organized; raises difficult questions; builds shared knowledge; builds social capacity; and finally, produces innovative responses" (p. 422). The electronic environment presents a medium in which these criteria may be addressed or fostered. E-participation allows public officials and citizens to engage in discourse in a controlled and evolving atmosphere. In essence, each instance of participation in an electronic format shapes future arrangements as the online community develops.

One of the primary goals for deliberative e-participation is breadth. In other words, it is necessary to support a wide participatory base in order to achieve the appropriate level of interaction, dialogue, and collaboration. Too few participants and too narrow of an interest spectrum leads to views and outcomes that may not be representative of the public base. Weeks (2000) argues that wider participation is a necessary feature if the development of a civic culture is one of the desired outcomes. It is equally important for the generation of public will and improving general discourse.

In order for deliberative e-participation to be effective, it must be credible as well as representative. It is not enough that a large number of citizens become part of the public discourse; in addition, the opinions and commentary provided must tenable. If they are not, then the legitimacy of the governance process and its outcomes are undermined. This supports the desirability and viability of well-planned and well-executed information exchange. The better informed the public is, the more credible their input.

One of the more interesting features of deliberative e-participation is the ability it has to inform future actions and decision making. Over time, repeated interaction and extensive dialogue will create a usable knowledge base that can be shared and drawn upon in a multitude of governance scenarios. In this way, social capacity is increased and decision making may improve with regard to both timeliness and innovation.

Facilitating E-Participation

It is clear that public participation is an important and desirable component of the governance process; the difficulty of creating and supporting e-participation is another matter. Civic participation as it exists today in the United States is rife with apathy. The disinterest in public engagement is further degraded by distrust of public officials, estrangement from public institutions, the complexities of life, and overall pessimism regarding government. While this would seem to be an untenable situation, there is reasonable optimism that the development of e-participation may offer new opportunities for enhancement of the existing system. However, one of the key challenges facing supporters of e-participation is the difficulty surrounding the creation of a welcoming and worthwhile environment in which the deliberative process can take place (Weeks, 2000). At its core, facilitating e-participation is a function of three things: technology, usage, and support. The information technologies must be viable and user friendly in order to promote usage, while concurrently, usage must be supported in order to foster expanded access.

Providing information and government services in an electronic format necessitates well-planned information systems. Public institutions must be prepared to provide data and services in an understandable and user-friendly format. This may include access by individuals with varying degrees of expertise, hardware that ranges anywhere from obsolete to cutting edge, multiple platforms, and possibly a multitude of languages. The goal is to use technology to reach a wider and more diverse audience. In order to achieve this, an array of technologies will be necessary.

Information Technology and E-Participation

A plethora of technologies is currently available for use as tools to facilitate e-participation. These technologies allow multiple levels of information delivery and communications, making it possible for citizens to interact with others and to engage in civic dialogue. Any discussion of technological tools must begin with the Internet and what have become our primary service networks: the World Wide Web (WWW) and e-mail. The Internet as a medium

provides a backbone of connectivity for both organizations and individuals. Via the Internet, municipalities create accessible and user-friendly Web sites, which allow information to be channeled to citizens as well as providing a conduit for service delivery, discourse, and civic engagement. Once an Internet presence has been established, it is possible to develop a wide array of e-government opportunities using one or more technological means. Following is a discussion of a few of these options.

E-mail is arguably the most extensively used application by individuals and organizations. It has become fundamental to doing business and communicating in our society. While it tends to be a one-to-one communications channel, it is a very versatile and user-friendly option for information delivery and general interaction. Mailing lists or list services offer another option for general delivery of information and provide similar applicability to that of e-mail while allowing for many-to-many communications. These lists are extremely stable forms of communication technologies and have been extensively utilized for over 10 years. Citizens may subscribe to a list, essentially self-selecting their participation channels.

While information delivery and general communication are necessary and fundamental to e-participation, further access is required to achieve interactive participation. Online databases and the forms associated with them are one such technology. Web forms come in a variety of types; they range from simple data input points to structured surveys. Through this medium, government can solicit various kinds of information and input from citizens regarding upcoming situations, decision points, or issues. Web forms also make it possible to archive responses and information into searchable databases. From an e-participation perspective, these are useful for future reference both by public officials and citizens alike.

Finally, information technology must support deliberative e-participation through the facilitation of active discourse. Chat rooms and discussion boards are the most common conduit for such engagement. Chat rooms allow for real-time interactions in all three formats: one to one, one to many, and many to many. These interactions may be scheduled by public officials or citizens in order to raise or discuss issues, converse about general topics of interest or concern, and simply chat about items that are of interest to the community at hand. Online chats have gained in popularity because they allow for communication at any time a group chooses and they approximate a conventional face-to-face interaction. This is one technology that is currently experiencing further advancements through the addition of video and audio capabilities, thus alleviating the need for advanced typing skills. It stands to reason that as the technology gets better, the communications capacity will improve right along with it.

Discussion boards or online forums are more linear, providing 24/7 engagement through threaded asynchronous communication. All discussions appear as posts to a particular topic or thread. Threads may be created and managed by either the public official or the citizen. Discussion boards are very viable for e-participation as they allow the user to come and go in the discussion, offer the opportunity to read through and ruminate on other's posts, allow for adequate time for individual consideration, and finally, the opportunity to modify input or remove it completely. Using this medium, the progression of the discourse may be tracked and the discussion can evolve based on the postings of the participants.

While these technologies are a limited representation of what is available to facilitate e-participation, they do offer a vision of what is possible. New opportunities for enhancing citizen involvement arise regularly as technological advancements are always on the horizon.

Beyond Technologies

E-participation is certainly not just a function of using the most viable information technologies; it is also a matter of providing the necessary support for the systems as well as promoting citizen usage. When developing e-participation strategies, it is important not to overlook the importance of access and user friendliness. Facilitating e-participation requires that the information systems and user applications function appropriately and are maintained so that access is not interrupted or problematic. It is important that citizens are not merely invited to be part of e-governance—they must also be enabled (Ward, 2005). These concerns go beyond the digital divide, shifting focus to designs that accommodate all users. Obviously it is not realistic to expect that any given system can include everyone, but care must be taken to make sure that there is no exclusion of any particular group.

System administrators must be aware of the diverse capabilities of the populous and design the systems to be interactive and user friendly. For many users, technology is still somewhat confounding. It is the job of government to help remove some of the mystery of the electronic medium, especially for those who typically find themselves behind the technological learning curve. As we progress in the information age, this becomes less of a problem. The demystification of the electronic medium is further advanced through user-friendly applications, effective training, as well as reliable and secure systems.

E-participation, especially deliberative e-participation, is relatively new and underutilized. At this juncture, it is very important that the public be supported, particularly as they become more familiar with electronic interactions. No one approach to the facilitation of e-participation will be sufficient. The needs of the populous are too diverse to allow for a one-size-fits-all method. To that end, public discourse and feelings of connectedness may be enhanced through customized applications.

Finally, usage becomes a significant concern for the development of e-participation. Part of facilitating e-participation must be a thorough reading of the needs and desires of the public. It is vital to try to include as many individuals as possible; it is in this way that a more representative group is developed. People who do not participate due to circumstance, physical challenges, and personal choice should be encouraged to access government through electronic means. Citizens must have a sense that they are a necessary and desired part of the public decision-making process—that they have a significant role to play in the development of virtual communities and government processes. Instead of a top-down approach, e-participation must support a bottom-up approach, which Mary Timney (1998) describes as government with the people, or in some cases even government by the people. This necessitates an environment where decision-making power is not centralized but distributed throughout the affected community. Allowing the public to inform governance is important to achieving an effective participation model.

Conclusion

All forms of participation can be valuable in the governance process because they bring individuals together. In essence, participation allows citizens to find out about diverse interests and how each is related to a common good. It redirects a portion of civic responsibility to the citizen: Individuals become part of the process, thereby allowing people to see themselves in a broader context. In an early work that discusses the impacts of technology on democracy, Abramson, Arterton, and Orren (1988) describe the value of direct participation in this way: "… by allowing citizens to act like citizens, participation acquaints each with the interest of all. Participation gives the citizen education in, and responsibility for, the common good" (p. 179). They go on to argue that a crucial consideration in this regard is the need for discourse: "Participation can deliver civic education and civic virtue only when it takes the form of deliberation and dialogue, persuasion and debate" (p. 179). The authors suggest that this requires activity beyond voting, which can be described mainly as the individual's assent of predetermined interests.

One of the tenants of improved participation in this country is the need to facilitate an engaged citizenry, that is, to get the public more fully involved in the process of decision making within their communities. Weeks (2000) argues that this approach necessitates that citizens have an opportunity to fully evaluate the issues at hand. This means that they must have access to reliable and legitimate information, a full view of the possible alternatives, and then the chance to make a judgment about what they believe to be the best option given all of the information.

E-participation has the potential to play multiple roles in the promotion of civic engagement. One possible outcome is the development of diverse virtual communities. E-participation has the ability to bring together diverse populations, previously disenfranchised citizens, and remote voices, thereby stimulating innovative dialogue around complex public issues. In addition, e-participation holds the potential to equalize some of the power most often associated with political power players and technical elites. The average citizen can access information and attain deeper understanding of the issues, allowing for more informed and higher quality civic discourse.

E-participation has the ability to organize like minds, forming a powerful base from which to engage in the decision-making process. Certainly, in a representative democracy there is power in numbers. Consequently, a large group with a cohesive and well-developed message may prove to be doubly powerful. E-participation could conceivably bring these individual voices together, allowing for those with similarity of interest to make their voices heard. No longer must interest demand proximity; electronic mediums allow like-minded individuals to create a community without boundaries. In order for this to happen, certain criteria must be present. E-participation systems must be well designed and supported by public officials. Citizen usage must be encouraged and supported. Also, the information provided must be clear, accurate, and accessible, and the e-participation environment must be open and well managed. Finally, decision makers must agree to use the medium and to respond as well as act based on what is found there.

If citizens are truly the owners of government in a real and active sense, then e-participation must facilitate the direct participation needed to allow this ownership to come to fruition.

References

Abilock, D. (2005). Six promising approaches to civic engagement. *CSLA Journal, 29*(1), 8-11.

Abramson, J. B., Arterton, F. C., & Orren, G. R. (1988). *The electronic commonwealth: The impact of new media technologies on democratic politics.* New York: Basic Books.

Al-Kodmany, K. (2000). Public participation: Technology and democracy. *Journal of Architectural Education, 53*(4), 220-228.

Carver, S., Evans, A., Kingston, R., & Turton, I. (2000). Accessing geographical information systems over the World Wide Web: Improving public participation in environmental decision-making. *Information Infrastructure & Policy, 6*(3), 157-170.

Cook, J. E. (1982). *The federalist.* Middletown, CT: Wesleyan University Press.

Dumbauld, E. (Ed.). (1955). *The political writings of Thomas Jefferson: Representative selections.* New York: Liberal Arts Press.

Garson, G. (2006). *Public information technology and e-governance: Managing the virtual state.* Sudbury, MA: Jones and Bartlett Publishers.

Hampton, K. (2003). Grieving for a lost network: Collective action in a wired suburb. *Information Society, 19*(5), 417-428.

Holman, J., & McGregor, M. (2001). "Thank you for taking the time to read this": Public participation via new communication technologies at the FCC. *Journalism & Communication Monographs, 2*(4), 159-202.

Hudson-Smith, A., Evans, S., & Batty, M. (2005). Building the virtual city: Public participation through e-democracy. *Knowledge, Technology & Policy, 18*(1), 62-85.

Innes, J., & Booher, D. (2004). Reframing public participation: Strategies for the 21st century. *Planning Theory & Practice, 5*(4), 419-436.

Kathi, P. C., & Cooper, T. L. (2005). Democratizing the administrative state: Connecting neighborhood councils and city agencies. *Public Administration Review, 65*(5), 559-568.

Macintosh, A. (2004). Characterizing e-participation in policy making. In *Proceedings of the 37th Hawaii International Conference on System Sciences.*

Morse, R. (2006). Prophet of participation: Mary Parker Follett and public participation in public administration. *Administrative Theory & Praxis, 28*(1), 1-32.

Noam, E. (2005). Why the Internet is bad for democracy. *Communications of the ACM, 48*(10), 57-58.

Osborne, D., & Gaebler, T. (1992). *Reinventing government: How the entrepreneurial spirit is transforming the public sector.* New York: Penguin Group.

Rosenbaum, N. M. (1978). Citizen participation and democratic theory. In S. Langton (Ed.), *Citizen participation in America* (pp. 43-44). Boston: Lexington Books.

Timney, M. M. (1998). Overcoming barriers to citizen participation: Citizens as partners, not adversaries. In C. S. King & C. Stivers (Eds.), *Government is us: Public administration in an anti-government era* (pp. 88-99). Thousand Oaks, CA: Sage Publications.

Ward, J. (2005). An opportunity for engagement in cyberspace: Political youth Web sites during the 2004 European Parliament election campaign. *Information Polity: The International Journal of Government & Democracy in the Information Age, 10*(3/4), 233-246.

Weeks, E. C. (2000). The practice of deliberative democracy: Results from four large-scale trials. *Public Administration Review, 60*(4), 360-372.

White, C. S. (1997). Citizen participation and the Internet: Prospects for civic deliberation in the information age. *Social Studies, 88*, 23-28.