White Paper

Balancing Mobility and Security

Bahar Barami
Senior Economist, DTS-24
Volpe Center
7617-4949-2150
barami@volpe.dot.gov

Prepared for:

Symposium on:
"Balancing Mobility and Security:
Innovative Approaches to Transportation Security"

Held at the Volpe Center
55 Broadway, Cambridge, MA
May 6, 2004

Overview

Is there an inexorable tradeoff between transportation mobility and security? Can we attain one only at the expense of the other? Or can both mobility and security be achieved as beneficial byproducts of advanced technologies embedded in the transportation network?

This paper reviews three common measures of mobility – accessibility, reliability, and affordability – and the methods used to assess and mitigate security risks, and suggests that at the nexus between security and mobility there are technologies that are common to both, with potential synergistic effects. The paper maintains that the associated tradeoffs are not between security and mobility, but rather between security and privacy, security and redundancy, and security and higher out-of-pocket costs to users. Note that whereas decisions to pay for security or transportation mobility both involve policy choices and tradeoffs, security decisions are far more difficult because the outcomes are harder to measure. It is impossible to specify analytically how much risk we should be prepared to take as a nation, or how much security is enough. The decision is ultimately a political one, and should be made through the political process. What we can do is to craft a public policy framework to address these tradeoffs. This symposium on "Balancing Security and Mobility" is an attempt to take steps towards identifying the criteria for evaluating the public and private choices between competing security and mobility improvements and the concomitant costs and benefits.[1]

Measuring and Enhancing Mobility

What is mobility? Has transportation mobility in the U.S. risen or declined? Is mobility an attribute of the transportation system or does it describe the people using the network? What are the indicators for measuring mobility?

By some indicators – metrics such as passenger or vehicle miles traveled, automobile ownership, trip length, affordability – levels of mobility enjoyed by Americans in the past century have grown exponentially. In the 40-years between 1960-2000, highway passenger miles grew nearly fourfold, from 1.3 trillion in 1960 to 4.4 trillion in 2000. Over the same period, highway vehicle miles grew more than threefold from 719 billion to 2.7 trillion (National Transportation Statistics, Figure 1.)

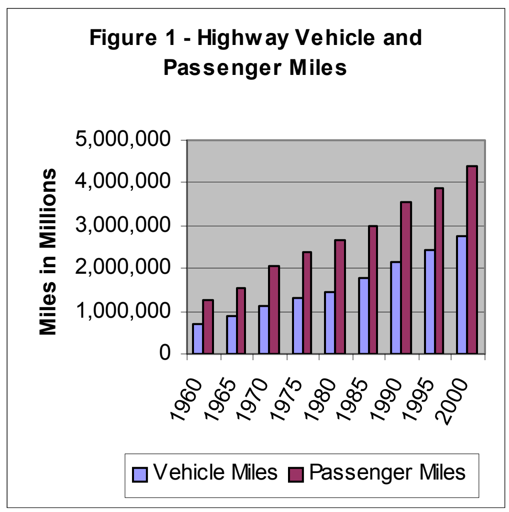


Figure 1 - Highway Vehicle and Passenger Miles

Source: National Transportation Statistics, 2002

In the nation's 75 major urban areas, passenger-miles of travel in have increased by more than 90 percent in the past two decades alone (Texas A&M University, 2003.)

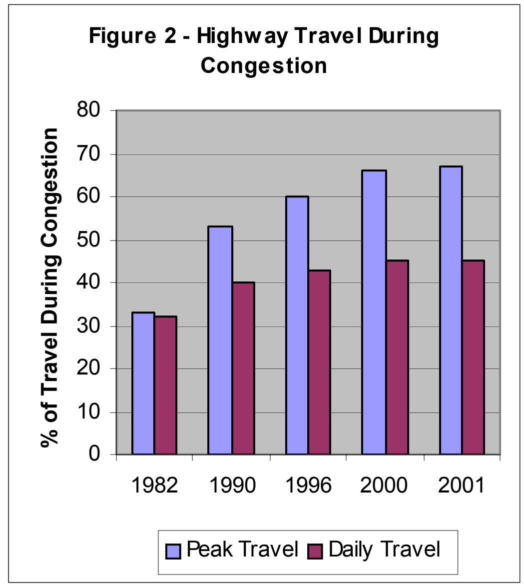
[1] Note that the term "tradeoff" in this paper is used synonymously with "opportunity cost" or simply "cost" as defined by the Nobel Laureate economist James Buchanan: "Any opportunity with the range of possibility that must be foregone in order to select a preferred but mutually excluding alternative reflects 'costs' when it is 'sacrificed.' And its rejection must involve *pain* despite the fact that differentially greater pleasure is promised by the enjoyment of the mutually excluding alternative." (Buchanan, 1969)

Also growing to a record high in the past decades has been another mobility indicator: average personal spending on transportation. Today, on average, households spend some 19% of their personal expenditures on transportation (second only to housing.) Affordability has also grown: for the first time in recorded census history, less than 10% of all U.S. households are reported to be without a vehicle (Pisarski, 2003.)

Are these good measures of mobility in the U.S.? Has American mobility grown in the past two decades?

The attributes of mobility are speed, cost, convenience, safety, and reliability, as Alan Pisarski, the prominent industry expert, put it in a testimony before a Congressional Committee for the reauthorization of TEA-21. To attain these objectives, he noted, "We invest enormous sums on transportation infrastructure and networks… and the product of that investment is mobility" (Pisarski, 2003.) Yet, there is a catch in this increased mobility: "Congestion is one of the prices we pay for a high degree of affluence and vehicle affordability," says Pisarski. Paradoxically, a decline in network mobility is a direct result of the steady increase in two key metrics for personal mobility: automobile ownership and trip making.

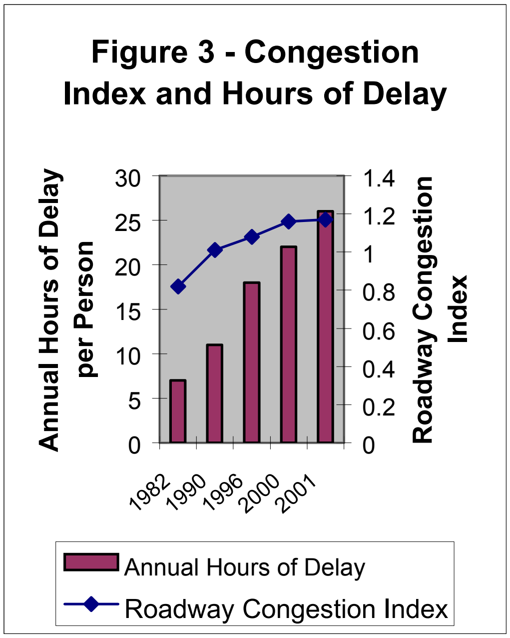
Congestion level is one common measure of the conflict between personal mobility and network capacity. The percentage of daily travel during congested highway conditions rose from 30% in 1982 to 45% in 2001, while peak period congestion during the same period grew from 33% to 67%. (Texas A&M University, 2004, Figure 2.)



Source: Texas A&M University, 2004

Other indicators of the disparity between highway capacity and passenger demand for personal mobility include Annual Hours of Delay and the Roadway Congestion Index.[2] Between 1982 and 2001, annual average delays for every person in the 75 urban areas studied by the Texas A&M congestion survey rose from 7 hours in 1982 to 26 hours in 2001. Roadway Congestion Index during the same period rose from 0.82 to 1.17 (Figure 3.)

[2] Defined as the ratio of daily traffic volume to the supply of roadway.



Source: Texas A&M University, 2004

DOT's Mobility Measures

Metrics such as passenger miles of travel or auto ownership measure personal mobility. But personal mobility can clearly be in conflict with network mobility. We need a corresponding measure for the mobility of the network where individuals travel. The DOT Strategic Plan fuses the two metrics for individual and network mobility. It uses the concept of mobility to articulate its goal for the transportation system: "*to shape an accessible, affordable, reliable transportation system for all people, goods, and regions,"* in support of which the Department intends to:

- Increase *access* to transportation system for the individual user
- Increase the *reliability* of trip times for the users.
- Reduce the *cost* of transportation for the users

Network and transportation systems are characterized not by "mobility" as such but rather by the three attributes of Availability, Capacity, and Efficiency. To meet the passenger mobility requirements, we need to ensure the network's:

- *Availability* to make it➔ Accessible
- *Capacity* to generate ➔ Reliable Trip Times
- *Efficiency* to make it ➔ Affordable.

The Federal Highway Performance Plan has treated all three passenger mobility criteria – accessibility, trip time reliability and affordability – as automatic byproducts of improved maintenance of the national highway system (NHS.) The Plan outlines a number of "strategic outcomes" which are achieved by maintaining the "physical condition" of the transport system and the NHS, which in turn lead to improvements that:

- Ensure the structural integrity of the pavement and bridges;
- Provide adequate lane capacity – which in turn reduces congestion, delays, and travel times for the individual users; and
- Reduce costs by lowering congestion levels and reducing the wear-and-tear on vehicles and fuel consumption.

While the Performance Plan addresses the maintenance requirements of the NHS — and the effects on capacity, structural integrity and user costs – it does not address the link between the NHS network capacity and security; nor does it address any links between security and user mobility.

What is the nexus between security and network accessibility/availability? Between security and network capacity/trip time reliability? Between security and efficiency /affordability?

Identifying the points of interface between security and each of these network/user attributes will help us reframe the questions as follows:

- Can security be attained only at the expense of mobility? If so, which attribute is most often traded off: access, reliability, or affordability? Or,

- Can both transportation mobility and security be obtained as byproducts of the advanced technologies embedded in the transportation system? Or

- Are the more relevant tradeoffs the ones we have to make between security and privacy; security and higher out-of-pocket costs; and security and lean logistics/efficiency (i.e., more infrastructure redundancy)?

The nexus between security and accessibility/availability

Accessibility, narrowly defined, describes access by mobility-restricted users and individuals. From a systemic perspective, however, accessibility relates to capacity availability, the essence of transportation service. Under some security threat conditions, system accessibility is an all-or-nothing attribute: making capacity available is a choice between shutting down the system or keeping it open but vulnerable, with no alternatives in between. Under this condition, the tradeoff of access and security is absolute. But under most circumstances the total system shutdown is treated as an extreme form of security precaution and access restrictions are only partial.

To illustrate, when the airports shut down in the immediate aftermath of September 11, the total system costs for the two day work stoppage and partial shut-down were estimated at $35 billion (Navarro and Spencer, 2001.) Similarly, shut downs at the seaports a couple of years ago on the West Coast were estimated to have cost the nation approximately $1 billion per day for the first five days, with the costs rising exponentially thereafter (Hart and Rudman, 2002.)

The high cost of the loss of access has in some contexts been referred to as the "security-service" tradeoff. The threshold for the point at which these costs begin to accrue is fairly low, as some analysts have pointed out: "The benefits of transportation in the United States stem from the ease by which travelers can move……To the extent that steps to reduce vulnerability to terrorism compromise personal and economic mobility, the mere threat of terrorism imposes significant social and economic costs on the United States" (Howitt and Makler, 2003.)

Dealing with the tradeoff of security and access is sometimes couched in terms of minimizing the costs of restrictions on commerce. The DHS Secretary Thomas Ridge, at a recent gathering of the trucking industry executives, remarked that one of his primary challenges was to "balance security and commerce;" goals that he regarded as "often conflicting." Secretary Ridge told the industry group: "Right after 9/11, we secured our borders all right, [but as a result] virtually no trucks were getting through from Canada and Mexico." The Secretary used curtailment of commerce as another metric for measuring the cost of restricting the mobility of cargo and transportation assets, clearly linking loss of access to transportation facility (i.e., shut down of borders) and the loss of benefits from commerce (i.e., the ultimate purpose of transportation, itself a "derived demand.") Secretary Ridge's comments on this particular occasion referred to the recent concerns of the trucking industry about the onerous requirements of the DHS for background checks on hazardous materials (HM) truck drivers. This requirement has compounded the existing access restrictions at the borders, as some 3.5 million drivers of trucks carrying HM are required to undergo background checks and fingerprinting by law enforcement agencies in the near future (Transport Topics, 2004a.)

Are there any methods available to secure the borders and ensure access to the network without shutting down or restricting the availability of the system's services? We know about the elaborate automated passenger and vehicle checks available at airports and land borders. How can these systems help mitigate some of the border security concerns? The new generation of the Computer Assisted Passenger Pre-screening (CAPPS II) promises to be an effective screening tool, as described by Admiral Loy: "Our effort is not to find a needle in a haystack but take the haystack off the needle" (New, 2003.)

Yet, concerns for privacy have restricted the range of applications for centralized databases and biometric devices to screen for access and border entry. For instance, many privacy concerns directed at the CAPPS II, including the one by the Reason Foundation (Poole and Passantino, 2003) have to do with the massive databases created from airline passenger information. Responding to such reports, the DHS Chief Privacy Officer Nuala O'Connor Kelly has stated that CAPPS II is in fact not a database, but a system for verifying passenger information: "The best thing and the worst thing I can say about this system is that it is not a database, and so the potential for misuse is almost nil" (Ballard, 2003.)

So, at the nexus between security and accessibility, some key tradeoffs are likely to be between accessible /available networks and unrestricted flows of commercial activity on the one hand, and confronting significant threats to security that are averted only at the price of losing privacy.

The nexus between security and congestion/network reliability

Congestion, in many contexts, is used synonymously with lack of mobility. The opening words of a December 2003 GAO study of the nation's ports and freight facilities directly link ports' "mobility" problems to congestion on the one hand, and the new security measures on the other:

> "The major challenges to freight mobility share a common theme – congestion……Freight mobility is most affected by congestion related challenges. Freight traffic on roadways has increased fourfold over the past two decades, and both rail and highway congestion are particularly severe in urban areas where container ports for international trade are located…..*Increased port security may exacerbate congestion if new controls drastically slow the movement of goods"* (GAO, 2003: pp 2-3, emphasis added.)

The GAO report adds that tighter security measures adopted in and around gateway ports, though another potential source of congestion, have not yet materialized as significant threats. The report, however, recognizes that future security measures – e.g., stricter container inspection and port access controls – could have a major impact on the flow of traffic at a freight facility. It cautions that "developing and effectively implementing future solutions that can accomplish security goals while still allowing efficient movement of goods, particularly at ports, is a matter of substantial concern," concluding:

> "Security and freight mobility are not mutually exclusive goals, but they can potentially conflict, adding to congestion. Access in and out of ports represents perhaps the highest potential for conflict between those two goals" (GAO, 2003.)

Going beyond the superficial causal linkages between elevated security concerns and higher congestion, we can identify some of the underlying problems and the corresponding solutions beneficial to both capacity and security. Both congestion and delays, for instance, can be reduced in a number of ways: adding capacity (new lane-miles), diverting passengers from the highway to transit modes, or investing in technologies – such as Intelligent Transportation System (ITS) – that enhance both capacity and throughput. But the same ITS technologies can also enhance security.

According to an ITS America document (ISTA, 2002,) ITS provides tools and enhanced opportunities to help safeguard the transportation system against a variety of threats, both natural and man-made, by:

⇒ Providing surveillance and analysis for freight and intermodal operations: monitoring and maintaining the security of containers on trucks and trains and in cargo handling facilities, monitoring other mobile assets, matching cargo against bills of lading, matching actual travel against intended routes and destination, and assuring the identify of commercial operations.

⇒ Proving surveillance and analysis for public transportation, including identification of and effective rapid response of threatening or high-risk passenger behavior, matching actual travel against planned routes and schedules, assuring the identify of transit vehicle operators, and proving surveillance and analysis at major transport centers.

⇒ Providing surveillance of other major transport facilities, including bridges and tunnels, and operations, management and response centers.

⇒ Safeguarding ITS systems and data (as well as other transport-related computer-controlled systems) against inadvertent or deliberate interference, destruction and misuse.

⇒ Providing logistical and communications tools to enhance the capabilities of transportation, law enforcement, defense, emergency response, and security organizations to plan and execute swift response, help rescue and treat the injured, clear roads and rails, smoothly reroute travel to available alternatives and restore services as possible, and provide the public with prompts and accurate information on transportation alternatives.

Advanced technologies are also effective for enhancing the transportation network's "reliability," with collateral benefits for both security and network capacity. In fact, many transportation studies have shown that network reliability and travel time predictability are far more critical to ensuring desired mobility levels than the conventional mobility measure of "speed." The Texas A&M team working on urban congestion has emphasized this key distinction when it pointed out that strategies that attempt to improve travel time – e.g., adding capacity or reducing the peak load through demand management and operational efficiency – are often not very effective for producing reliable travel times. Most of our computerized simulation and planning tools are not equipped to fully handle the importance of reliability, the team points out. The efficiency loss resulting from using average-speed data to calibrate traffic simulation tools is compounded by the fact that a significant amount of congestion data relates to averages based on fairly good traffic conditions – mid-weekday, clear weather and pavement, no collisions or lane-blocking roadwork, etc. – rather than the realistic conditions travelers and shippers need to allow for on-time arrival. Travelers value predictable travel time a great deal more than the average network-time. Yet, our tools are based on average network speed. This is an area where the shared objectives of security and mobility are likely to generate beneficial technology innovations.

Strategies for improving trip-time reliability are highly effective in reducing the amount of irregular problems that influence travel time. Only a few of the ITS User Service Bundles and User Services have clear security focus, yet many of them have potential applications for both security and capacity management. [*See the companion White Paper prepared for this Symposium by Joe Koziol entitled "Innovating ITS Technologies with Joint Security and Mobility Benefits.*] According to the Texas A&M congestion study, incidents – e.g., collisions, breakdowns, lane blockages – as well as disruptions due to work zones, weather, special events and traffic control problems are the primary causes of fluctuation in travel time. The ITS-based freeway incident-management programs attempt to make travel times more reliable by using traffic management tools used in conjunction with surveillance cameras and cell phone-reported incident call-in programs. By installing closed-circuit cameras, these call-in monitoring stations enable the response to incidents to be more targeted, and often reduce the total delay by shortening the time to detect a disabled vehicle. The programs also coordinate with the local emergency response teams, freeway service patrols and tow truck operators to further improve the incident management process. Incident Management programs have the added benefit of reducing "secondary crashes" – i.e., collisions within the stop-and-go traffic caused by the initial incident. Studies on the effectiveness of these tools have generated benefit-cost ratios between 3:1 and 10:1 for such programs (Texas A&M University, 2004.)

The Texas A&M study highlights the choices and tradeoffs involved in most public policy decisions by listing the array of alternative actions required to stop the growth of congestion:

> "The traffic growth rate in one year would have required 1,725 new lane-miles of freeway and 2,475 new lane miles of streets – OR – on average six million additional new trips per day taken by either carpool or transit – OR – operational improvements that allow three percent more efficient travel on the existing non-motorized or electronic means. [The study notes that this level of solution was not implemented in most regions, nor was any combination of such actions undertaken to enhance the improvement levels" (Texas A&M University, 2004.)

The critical nexus between security and congestion-management technologies – surveillance, monitoring and control and communications devices – clearly illustrates that security assurance and capacity enhancement are not zero-sum games. Many such technologies generate joint benefits. The problem is not the incompatibility of security and capacity objectives, but rather our ability to understand the full scope of the tradeoffs – privacy as well as other factors such as pricing, funding priorities, and mode choice.

The nexus between security and affordability/user-cost

Are we willing to pay more to be more mobile? Or pay the same to be more secure but a little less mobile? Or pay even more to gain both in security and mobility? This is how the willingness of the American motorists to pay for mobility is described by Anthony Downs, the Brookings Institution transportation expert:

> "Urban travelers pay for congestion by sitting in traffic: this is the price that Americans are willing to pay for the benefits that they derive from the urban activities that cause congestion (quoted in Pisarski, 2002.)

If there are any tradeoffs between having more affordable transportation or funding more security projects it is because we don't live in a world of unlimited resources. It is not because of their irreconcilable requirements that we have to trade off some mobility for more security, but rather because of the limited resources and the nature of political processes required to fund such projects.

Markets fail when it comes to paying for either mobility or security. This is because both security and mobility are "collective" or "public" goods. Market-based pricing mechanisms fail to produce adequate levels of collective goods, partly because of the free-rider problem: non-payers cannot be excluded from enjoying the product. For instance, consumers who don't value airline security or un-congested (but toll-free) highways don't pay a discounted price to travel. Markets also fail when they have to decide how much of the collective goods to produce or consume. For instance, the decision on the optimal level of vehicle throughput or cargo screening cannot be left to the private sector, partly because both transportation infrastructure and threats to homeland security represent a class of goods generating externalities – both positive and negative. So the financing of both transportation and security products are often done outside the normal financing schemes, through budgetary processes and taxation. (See Musgrave and Musgrave, 1973.)

Touching on the failure of free markets to ensure adequate investment in security is the DHS Secretary Tom Ridge who has commented on the difficulties of enlisting business cooperation in staving off terrorist threats, and on how hard it is for the government to institute standards for businesses in their conduct of security, concluding that: "The 'miracle of the marketplace' won't necessarily solve all these problems" (*Business Week*, 2002.)

Affordability of transportation or security is thus not a personal finance issue, but rather part of an elaborate political process for funding public projects. In fact, deciding what security projects to fund is not unlike the decision for funding major transportation projects. Available resources are not unlimited. A mechanism for prioritizing among candidate projects needs to be developed. Some of the techniques assess the benefits and costs, the risks and payoffs for each project. Other strategies use the political process for allocating resources. As a recent Brookings Institution report has pointed out, by devising an investment evaluation framework that would arrive at a cost-effective homeland security agenda, we could ensure that each additional dollar of spending is directed to achieving the greatest benefits in lives saved, costs averted or future attacks averted (O'Hanlon, et. al., 2002.)

Many researchers have maintained that because of the political mechanisms we use to fund major transportation projects, reduced investment in mobility is the price we pay for more security. Among these are Harvard University's Altshuler and Luberoff, who have reviewed the evolution of infrastructure investment policies in the U.S. in the post-Intrastate-Highway era (Altshuler and Luberoff, 2003.) In the past three decades, they maintain, there has been a general trend towards the diffusion of federal spending, as a result of which the nation's mobility/capacity needs have for the most part been trumped by environmental and neighborhood resistance – what the authors term the "do-no-harm" imperative. During this period, levels of congestion declined or remained stable, while mobility measures improved: A majority of Americans was able to travel farther, faster, more frequently, even in the face of funding cuts. These improved levels of mobility were achieved by exploiting space capacity already available (e.g., by moving from the city to suburb) and making capacity improvements through optimization measures such as peak spreading and traffic signal management.

Today, in the post-9/11 period, maintain Altshuler and Luberoff, the tradeoffs of security and mobility are real: in addition to the 'do no harm' environmental restrictions, investments in large infrastructure projects are likely to suffer because priority is given to security enhancements. They see clear tradeoffs between these two types of projects. In today's insecure climate, they say, security is achieved at the expense of large infrastructure projects. The effect of this tradeoff, they maintain, is compounded by the deteriorating public funding conditions triggered by the recent economic slowdown, the bursting of the technology bubble, and the combined effects of tax-cuts and budget deficits (Altshuler and Luberoff, 2003.)

Perhaps it is fair to say that our methods of funding public projects, compounded by our unwillingness to raise user fees, are the constraints jointly shared by both types of project: security and mobility. It is not their inherent incompatibilities that keep security and transportation capacity as rivals for funding, but rather the shared impediments: the decision processes used to fund public goods.

Policy Issues: Seeking the optimal level of security and mobility

When it comes to the choice between securing our borders and protecting our vulnerable infrastructure <u>or</u> enhancing our network capacity, we're not dealing with a zero-sum game. Today's advanced technologies allow us to do both. The choice is rather among other competing priorities: keeping user-fees low, avoiding privacy intrusions, and avoiding redundant controls and safeguards.

Today's advanced technologies – surveillance, satellite location and tracking, detection and sensing devices, and command and control systems – offer the capability for attaining full domain awareness. Many of these technologies allow us to embed security in every aspect of the infrastructure to achieve the real-time transparency of the assets. By enabling us to harden the vulnerable infrastructures, connect the system players and sub-segments, and monitor in real-time the network functions, these technologies have the potential to achieve both goals: enhance network capacity and ensure its security and continuity of operations.

What keeps us from achieving these goals?

The impediments may ultimately arise from the tradeoffs that are not between having more mobility or security, but rather between:

⇒ **Trading off some privacy to have more of both mobility and security.** Today's advanced communications, navigation, sensing, identification and control technologies have proven indispensable not only for managing the transportation network, but also for security functions needed for passenger screening, background checks, location tracking, and surveillance and movement monitoring. One major impediment to expanded use of these technologies is the price we pay in terms of the loss of privacy. How much privacy are we willing to tradeoff for a perfect domain awareness to help our traffic managers as well as the port-of-entry security personnel? As a nation we need to address this critical tradeoff more explicitly and systematically.

⇒ **Trading off more out-of-pocket fees, taxes and tolls for more network capacity as well as security.** We can reduce congestion by building a lot more capacity in the system, but are we willing to pay for them by raising the needed revenues? We can also upgrade our critical infrastructure to make them a lot more secure. But who should pay for the improvements? Are we willing to pay higher taxes, fees, and tolls, or do we prefer to play a shell game: shift the burden to others – private industry, other federal services, and state and local governments?

Pivotal to the questions of who should pay is a clearer notion of the role of the government and a better delineation of the role of the private sector. We also need to offer a wider range of financing options to help finance large-scale transportation infrastructure projects that generate both public and private benefits. As the previously mentioned GAO study has pointed out, the issue of who pays for improving congestion and security at freight facilities is still unresolved, and that as a nation, we need to determine the appropriate federal role, the report maintains, in order to lower the costs of providing and maintaining the infrastructure. The report points out that compounding the impact of security measures on freight infrastructure are the public sector processes at the state and local levels that are not suited for freight – partly because of the private sector ownership, and partly because local planners have not applied rigorous evaluation approaches such as Benefit-Cost Analysis (GAO, December 2003.) Identifying the private sector beneficiary of system improvements and promoting the private-sector participation to deploy dual-use applications for security and mobility are critical to avoiding some of the zero-sum tradeoffs.

⇒ **Trading off some efficiency for a greater degree of redundancy and slack in the transportation network in order to help build a more *resilient* system.**

Building redundancy would require not only a layered strategy for deploying security countermeasures, but also redundant assets and infrastructures. Yet we fear that if we adopt a risk management strategy based on building resilience, robustness, and redundancy in the transportation network we will automatically tradeoff a significant level of operational efficiency. For decades we have strived to keep costs down by reducing duplication and achieving lean inventory-control and pull-based supply chains. Yet the hidden costs here might be the loss of resilience. [*This issues is treated at a greater length in the companion paper for this symposium by Bahar Barami on "Survivable Transportation: Embedding Security into an Efficient Passenger and Freight System.*]

⇒ **Trading off some urban and suburban amenities to be more secure**. Another reason modern technology has failed to offer us maximum levels of mobility has been the choices we have made when designing and financing our vast urban transportation infrastructure. We have not been willing to reduce the high price of urban mobility by driving fewer miles or using more transit. Many of these choices have not been conducive to maximizing network capacity and optimal mobility levels. As the authors of the Texas A&M congestion study have conclude, over the past 20 years, traffic volumes have increased faster than road capacity. But our new technologies and innovative capacity management strategies have failed to provide the needed relief, partly because other factors such as jobs and schools have been competing for transportation investment:

> "Urban residents trade off a variety of factors and cost elements in the search for the best situation…realizing that these tradeoffs are made across a spectrum that might best be represented as several niche markets, rather than one or two large ones …. Building more roads is only part of the solution" (Texas A&M, 2004.)

In conclusion, the tradeoffs of security and mobility should ultimately be viewed in the context of a broader range of choices we need to make as a nation. Homeland security strategies need to promote a system-wide perspective for planning and financing the entire critical infrastructure. Today's advanced technologies will enable us to avoid the tradeoffs of having more security only at the expense of less network capacity, but we have not been able to enjoy the full benefits of these technologies for a number of reasons. Clearly some of the reasons have to do with our choice of urban lifestyle. The others have to do with our unwillingness to pay the price to be more secure, in this case the intangible price paid by giving up some privacy.

Nor are we willing to pay the price in terms of the economic resources needed to meet our security and mobility needs. To have more of both, we'd have to give up the alternative uses of more of the resources which would otherwise be put to other, perhaps more valued uses. And finally, there is a price we'd have to pay in terms of foregone efficiency. This is a price we'd pay by giving up some supply chain and infrastructure design efficiency as we build redundancy and slack in the system.

How do we assess all these tradeoffs? The answer lies in the decision processes we use for evaluating public policy and transportation investment options. It ultimately has to do with how we assess the risks we face and the public decision processes we pursue to design, fund, secure, and maintain the nation's critical infrastructure.

Bibliography

Altshuler, Alan, and David Luberoff, *Mega Projects: The Changing Politics of Urban Public Investment, Brookings* Institution Press/Lincoln Institute of Land Policy, 2003

Ballard, Tanya, May 30, 2003, "Report says proposed passenger screening system flawed and invasive," Government Executive Magazine.

Buchanan, James M. , 1969. *Cost and Choice: An Inquiry in Economic Theory*, The University of Chicago Press.

Business Week, June 10, 2002, "America's Biggest Job: Is the U.S. any less vulnerable to terror these days?"

GAO, December 2003. "Freight Transportation: Strategies Needed to Address Planning and Financing Limitations," Report to Committee on Environment and Public Works, U.S. Senate, GAO04-165.

GAO 2002. Statement of JayEtta Hecker, Director, Physical Infrastructure, July 02, "Homeland Security: Interagency Coordination and Partnership Will Be Critical to Success."

Hart, Gary, and Warren B. Rudman, 2002, "America Still Unprepared – America Still in Danger," Report of an Independent Task Force Sponsored by the Council on Foreign Relations.

Howitt, Arnold M. and Jonathan Makler, November 2003, "Protecting America's Highways and Transportation System Against Terrorism," Final Report for the TRB Annual Meeting.

ITS America, September 2002, "Homeland Security and ITS," available on www.itsa.org

Musgrave, Richard A. and Peggy B. Musgrave, 1973, *Public Finance in Theory and Practice,* McGraw-Hill Book Company, Second Edition.

National Transportation Statistics, 2002.

Navarro, Peter and Aaron Spencer, 2001. "September 11 Report: Assessing the Costs of Terrorism," The Milken Institute Review, Fourth Quarter.

New, William, April 17, 2003, "Transportation official seeks business advise on security," Federal Executive Magazine.

O'Hanlon, Michael E, et. al., *Protecting the American Homeland: A Preliminary Analysis,* Washington, D.C., Brookings Institution Press.

Pisarski, Alan, May 21, 2001, "The Meaning of Mobility," Slide Presentation, Eno Foundation.

Pisarski, Alan, March 19, 2002, Testimony before the US Senate, Committee on Environment and Public Works, "Mobility, Congestion and Intermodalism."

Poole, Robert W. Jr., and George Passantine, May 2003, "A Risk-Based Airport Security Policy," Reason Public Policy Institute, Policy Study 308.

Texas A&M University (2004). *2003 Urban Mobility Report*, accessed March 2004, http://mobility.tamu.edu/ums/report.

Transport Topics, "Security, Commerce Need to Be Balance, Ridge Says," February 16, 2004.