CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES | Homeland Security and Counterterrorism Program

July 31, 2013

Innovative Immigration and Border Control Reform

Stephanie Sanok Kostro and Scott F. Mann

Introduction

Over the last 10 years, the United States placed great emphasis on securing its borders and improving its immigration process. Concerns about terrorism in the shadow of the September 11, 2001, attacks led to the creation of the Department of Homeland Security (DHS) as a means for streamlining and improving the government's ability to protect the United States, its citizens, and its infrastructure inside the nation's borders. From intelligence gathering and sharing to interdiction and apprehension, the goal was to bring all of the essential homeland security agencies into one federal department and reduce the characteristically disparate and disconnected nature of previous homeland security agencies and responsibilities. Despite attempts to improve efficiency and efficacy, regulating the U.S. border and enforcing U.S. immigration policies remain significant challenges. The complexity of operations required to achieve the stated policy goals of the U.S. government, combined with the sheer volume of border traffic (licit and illicit, human and trade), hampered past attempts at effective border control, and cloud the potential for success of future operational undertakings.

The way an agency operates is an expression of the technologies available when it determined its requirements—including capabilities and processes—to execute its mission. For over a decade, the border components have placed a great emphasis on the application of technology to their business challenges. While many of these technologies have been deployed to automate and facilitate traditional ways of doing business, high-impact innovation requires more than simply streamlining business processes, and new technologies often offer entirely new possibilities for alternate ways of doing business.[1] This paper examines the potential to use current and emerging technologies to design and implement *new, innovative* ways of achieving border and immigration objectives.

To improve the efficiency of current operations, alleviate pressure on manpower in the border and immigration forces, increase the accuracy of detection and apprehensions, and simplify information gathering, technology offers myriad possibilities to enhance, and in some cases reinvent, border security and immigration procedures. While the future seems limitless, budgets are not. The U.S. government and its partners in innovation must be mindful of the financial limitations inherent in any government projects.

The first section of this paper examines the four core challenges to any border security and immigration reform effort. These include: (i) effectively controlling the physical U.S. border, which includes preventing unauthorized crossings; (ii) facilitating and enforcing terms of authorized entry, which requires maintaining accurate entry and exit records; (iii) implementing and enforcing internal compliance mechanisms such that individuals cannot realize economic benefits of unauthorized presence; and (iv) facilitating access to U.S. government-provided entitlements, rights, and benefits. To be successful, any reform movement must adequately address these essential elements.

The second section of this paper then examines the ways in which technology can address these challenges, including: security improvements; identity management; information sharing; and resource maximization. Current technologies, used in novel operational practices, could provide the means necessary to successfully address all four core challenges to U.S. border security and immigration reform efforts.

This paper reflects discussions from a February 2013 conference that featured leading experts from across government, industry, and academia on technological innovation and border and immigration reform. Both the conference and paper were made possible by the generous support of CSC, Ping Identity, and Equifax Inc.

[1] W. Brian Arthur, *The Nature of Technology: What It Is and How It Evolves* (New York: Free Press, 2009), 192–93.

Current Challenges

While the four core challenges—border control, compliance with terms of entry, internal compliance mechanisms, and facilitation of access to government entitlements, benefits, and rights—are replete with obstacles that have prevented them from being effectively addressed in the past, each challenge can be tackled through the innovative orchestration of current and emerging technologies. This section will analyze these core challenges individually and outline some of the key initiatives that have been used to confront them. It should be understood, however, that from a functional perspective, these core challenges are very much intertwined and interdependent. The success of one depends on the success of the others.

Border Control

Border control entails two somewhat disparate missions: enabling the efficient movement of goods and people, and preventing the entry of undesirable or ineligible individuals and items.[2] The nearly 7,500-mile U.S. border, coupled with 12,383 miles of coastline,[3] represents myriad possible legal and illegal entry points into the United States. Responsibility for securing the land and maritime borders falls to U.S. Customs and Border Protection (CBP) and the U.S. Coast Guard, respectively.

In any given year, nearly 350 million people enter the United States, the vast majority of whom are U.S. citizens.[4] In fiscal year 2012, CBP facilitated $2.3 trillion in trade through U.S. ports.[5] Modern border protection has sought to manage these massive cross-border flows by "pushing information-gathering and traffic control abilities away from the geographic border to areas in foreign countries and internally in the United States."[6] For example, U.S. consulates and the visa application process often serve as the first stage of border control. They begin identity verification and border screening long before a traveler reaches the actual geographic border, and establish the first layer of a multilayer defense against dangerous individuals. Similarly, the Container Security Initiative works with partner governments to inspect high-risk cargo at foreign ports before they depart for the United States.[7] Both of these processes expand the realm of border protection and create the additional security barriers of time and physical distance from the United States, improving CBP's ability to prevent or interdict undesirable or ineligible individuals or items attempting to enter the country.

Controlling the border requires the ability to secure open border areas and the capacity to effectively regulate designated ports of entry (POEs). For the former, the United States undertook a number of initiatives, such as constructing fences, erecting remote monitoring and surveillance stations, and increasing the workforce. For the latter, security at POEs requires the ability to verify the identities of entrants to the United States, connect these identities to the rights or benefits that adhere to U.S. citizenship or foreign national visitors, and screen for those entering without authorization, those who pose threats (e.g., members of terrorist or criminal organizations), or those who are otherwise undesirable or ineligible. Over the past decade, DHS pursued several avenues to streamline the entry process, while simultaneously increasing the accuracy of identity verification to detect threats. Some notable initiatives include the land border "NEXUS and SENTRI … registered-traveler programs in which frequent travelers enroll by submitting biometric and biographic information for criminal and terrorist background checks."[8] These programs distribute radio frequency (RF) ID cards (NEXUS) or equip

---

[2] U.S. Customs and Border Protection, "Priority Trade Issues," http://www.cbp.gov/xp/cgov/trade/priority_trade/; and Rey Koslowski, *The Evolution of Border Controls as a Mechanism to Prevent Illegal Immigration* (Washington, DC, Migration Policy Institute, February 2011), 8, http://www.migrationpolicy.org/pubs/bordercontrols-koslowski.pdf.

[3] U.S. Department of Commerce, U.S. Census Bureau, *Statistical Abstract of the United States: 2012* (Washington, DC: U.S. Department of Commerce, 2012), 225, http://www.census.gov/prod/2011pubs/12statab/geo.pdf

[4] Jayson Ahern, "Innovative Immigration and Border Control Reform" (panel discussion at conference on "Innovative Immigration and Border Control Reform," CSIS, Washington, D.C., February 7, 2013), http://csis.org/event/innovative-immigration-and-border-control-reform.

[5] Michael J. Fisher and Kevin McAleenan, "What Does a Secure Border Look Like?," testimony before the Subcommittee on Border and Maritime Security of the House Committee on Homeland Security, February 26, 2012, http://docs.house.gov/meetings/HM/HM11/20130226/100300/HHRG-113-HM11-Wstate-FisherM-20130226.pdf.

[6] Chad C. Haddal, "People Crossing Borders: An Analysis of U.S. Border Protection Policies," Congressional Research Service, May 13, 2010, 20, http://www.fas.org/sgp/crs/homesec/R41237.pdf.

[7] U.S. Department of Homeland Security, "Container Security Initiative Ports," http://www.dhs.gov/container-security-initiative-ports.

[8] Koslowski, *The Evolution of Border Controls*, 13.

cars (SENTRI) with RF chips that can be read at border checkpoints and pass along key biographical information.[9] Biometrics ensure individual uniqueness within the program, and create a tight physical connection with the traveler's biographic information. This mechanism expedites the entry-exit process and facilitates the collection of information regarding an entrant's visa adherence. Similarly, the Global Entry program collects biometric data of frequent travelers to use at airport POEs to make the entry process faster and more efficient.[10] These trusted-traveler programs (TTPs) do not eliminate the prerogative of border security officials to randomly screen travelers at the border area. By prescreening individuals before they reach the border, however, such programs allow low-risk travelers to move more quickly through the inspection process. TTP strengths include the development of biometrically anchored, trusted identity claims that provide the confidence to allow agencies to rely on automated screening and watch-list checks. The TTPs' weaknesses include their limited size and restricted availability, often only to citizens of select countries. As a result, they currently have minimal impacts on cross-border flows. Nevertheless, these programs are significant for their attempts to harness technology to improve the efficiency of transnational travel.

Compliance with Terms of Entry

The challenges of border control neither begin nor end at the physical border. One key aspect of effective immigration policy and border security is ensuring individuals adhere to the terms of their visa once they enter a country. Visa compliance in the United States is particularly troublesome, especially with regard to the basic condition of the period of authorized stay. Enforcing compliance with terms of entry requires an effective entry/exit system that accurately and efficiently indicates whether a visa holder remains in the country beyond the term authorized. Having a record of an individual's compliance with a basic condition of entry provides a reputational indicator that can be used to adjudicate future visas or immigration benefits. It also improves internal enforcement procedures and immigration integrity by alerting law enforcement of a visitor's unlawful presence for investigation. Ideally, both the government and the visa holder would be notified as a visa's expiration approaches.

At least two past U.S. initiatives aimed to address overstay violations. The original effort began in the 1980s and involved the creation of the I-94 form, a paper form intended to record a visitor's entry and exit information. However, due to the inherent weaknesses of I-94 paper data collection, records were often incomplete and thus unreliable. Subject-matter experts note that "due to lost forms, incomplete or inaccurate data entry, exit by land border, and incomplete deployment of the system, missing exit data corrupted the database, leaving immigration inspectors with no effective way of knowing if individuals had overstayed their visas."[11] Post-9/11 reform efforts led to the creation of the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program, which aimed "to establish a single identity for all individuals who interact with any immigration and border management organization by capturing the individual's biometrics, including 10 fingerprints and a digital image, at the earliest possible interaction."[12] This program, while promising, has lagged in its implementation. According to the U.S. Government Accountability Office, the comprehensive use of US-VISIT during entry procedures has not been matched in the exit process, thus making it useless for monitoring visa adherence for visitors.[13] This is in spite of a statutory requirement that DHS develop and implement an exit-monitoring program. "DHS has not yet implemented a comprehensive biometric system to match available information (e.g., fingerprints) provided by foreign nationals upon their arrival and departure from the United States and faces reliability issues with data used to identify overstays."[14] Without the implementation of an effective exit-monitoring process—biometric or otherwise—the enforcement of visa compliance will remain elusive.

---

[9] Ibid.
[10] Ibid.
[11] Ibid., 14.
[12] U.S. Government Accountability Office, "Homeland Security: Strategic Solution for US-VISIT Program Needs to Be Better Defined, Justified, and Coordinated," February 2008, 2, http://www.gao.gov/assets/280/272939.pdf. US-VISIT has been renamed the Office of Biometric Identity Management (OBIM).
[13] Ibid.
[14] Richard M. Stana, "Visa Security: Additional Actions Needed to Strengthen Overstay Enforcement and Address Risks in the Visa Process," testimony before the Subcommittee on Border and Maritime Security, House Committee on Homeland Security, September 13, 2011, http://www.gao.gov/new.items/d11910t.pdf.

Of course, temporal limitations associated with visas are not the only conditions that require enforcement mechanisms. Perhaps even more important is the matter of ensuring that the permission to enter is used within the limits agreed between the government and the beneficiary. In short, the challenge is to prevent an authorized entry for the purpose of tourism from being leveraged into unauthorized residence and employment. This has caused policymakers to focus on the major pull factor of illegal immigration—jobs and economic rewards. Yet workplace enforcement—largely dependent on resources available to Immigration and Customs Enforcement (ICE) for investigation into employment situations and for removal of unauthorized workers—is another vexing immigration and border-control challenge.

Internal Compliance Mechanisms

The third challenge is internal compliance mechanisms, most critically workplace enforcement. The attraction to enter, and the incentive to remain in, the United States illegally is a product of market demand: the ability to realize economic and social benefits from such presence without consequence. If the United States could reduce the demand, or make it increasingly difficult to attain economic benefits, the supply will dry up. A Pew Research Hispanic Center study from 2010 noted that the number of new illegal immigrants fell between 2007 and 2010, a decline that correlates with, and was likely a result of, the financial crisis and recession.[15]

Several efforts aimed to decrease the demand for illegal immigration. Requirements such as the I-9 form, a paper employment verification system established by the Immigration Reform and Control Act of 1986 (IRCA),[16] were important early steps. However, the I-9 simply required employers to review one or more documents to verify a new employee's eligibility to work in the United States and was thus "highly vulnerable to fraud."[17] Like its I-94 cousin discussed above, this 1986 paper solution is a good example of how technology at that time (essentially, paper forms and various physical credentials) bounded the process to address the business requirement. The updated version of the I-9 is known as E-Verify, which utilizes much of the same information on the I-9, but cross-checks the data through numerous government databases to verify an applicant's provided identity and work eligibility documents.[18, 19] Again, E-Verify is a reflection of commonly available technology circa 2003: internet browsers, federated query capabilities, web services. These capabilities shifted a business practice in which it was impractical to verify the information provided on a paper I-9 form, to one in which the data on the physical credentials could be automatically compared to original sources and provide a near-instant confirmation to the employer.

Participation in the E-Verify program has grown quickly. In 2005, just 5,900 businesses had enrolled. By 2012, the program had increased to 418,000. Accordingly, employer queries grew from 1 million in 2005 to 20.1 million in 2012.[20] Still, those numbers are a mere fraction of the nearly 7.4 million businesses in the United States.[21] Because E-Verify remains small and mostly voluntary and because the process verifies documents rather than linking a presented document to a trusted identity, it has a limited ability to prevent illegal employment. Identity fraud remains a critical weakness with the employment verification process.

Further, for E-Verify to fulfill its legislative intent, initial screening must be followed up by enforcement. Again, however, ICE has "limited resources to investigate and sanction employers that knowingly hire unauthorized workers or those that knowingly violate E-Verify program rules. Instead … ICE agents seek to maximize limited resources by applying risk

---

[15] Jeffery Passel and D'Vera Cohn, "Unauthorized Immigrant Population: National and State Trends 2010," Pew Research Hispanic Center, February 1, 2011, http://www.pewhispanic.org/2011/02/01/unauthorized-immigrant-population-brnational-and-state-trends-2010/.
[16] Doris Meissner and Marc R. Rosenblum, "The Next Generation of E-Verify: Getting Employment Verification Right," Migration Policy Institute, July 2009, 1, http://www.migrationpolicy.org/pubs/verification_paper-071709.pdf.
[17] Ibid.
[18] Ibid., 4.
[19] It is important to note that E-Verify's "identity check" is more properly described as a verification of the data on the "identity" credential. It is a document check that depends on the employer to make the critical determination whether the "identity" truly belongs to the individual presenting it.
[20] Ruth Ellen Wasem, "U.S. Immigration Policy: Chart Book of Key Trends," Congressional Research Service, March 7, 2013, 13, http://www.fas.org/sgp/crs/homesec/R42988.pdf.
[21] Ian Simpson and Vicki Allen, "Number of U.S. businesses fell in 2010: Census Bureau," Reuters, June 26, 2012, http://www.reuters.com/article/2012/06/26/us-usa-economy-businesses-idUSBRE85P0X720120626.

assessment principles to worksite enforcement cases and focusing on detecting and removing unauthorized workers from critical infrastructure sites."[22] While perhaps necessary from a budgetary and resource perspective, such a piecemeal approach to enforcement does little to deter violations.

Finally, implementation of E-Verify on a broader scale remains a challenge. Caused by downstream data-quality problems,[23] false nonconfirmation of legal workers creates issues for both U.S. workers and U.S. businesses.[24] The expansion of the program beyond biographic data to include biometric identification is one potential solution[25] because it could address the problem of connecting individuals with the credentials that establish their ability to work in the United States and would prevent false nonconfirmations that often occur due to biographical data discrepancies. Unlike the US-VISIT implementation of biometrics at key government locations (e.g., POEs and embassies), the notion of proliferating government-required biometric readers throughout the U.S. business community is a nonstarter. Making biometrics more widely available will require innovative ways of deploying and using the technology.

Facilitation of Access to Government Entitlements, Benefits, and Rights

Residence in the United States can yield access to certain entitlements, benefits, and rights, such as social safety nets, health care, as well as legal protections. These increase the value of residing and remaining in the United States, including unlawfully. One of the core challenges facing the United States is ensuring that those who are eligible to access these benefits can receive them with limited hassle and few restrictions, while preventing those who are ineligible from accessing them. This requires an efficient and effective process to connect a credential that stipulates such benefits with the individual claiming them. Currently, federal and state laws are a maze of provisions, restrictions, and exceptions regarding access to entitlements and benefits. The Systematic Alien Verification for Entitlements (SAVE) system "provides federal, state, and local government agencies access to data on immigration status that are necessary to determine noncitizen eligibility for public benefits."[26] Still, the process is highly manual, vulnerable to identity fraud, and subject to inaccuracies that prevent the right result.

Formidable challenges remain for effective border and immigration reform. Very few of these challenges are new and they have common issues. All are in need of efficient processes to gather and verify fraud-resistant data. By reimagining the business operations made possible by current and emerging technologies, innovation offers promising possibilities for a new era of border control and immigration.

Changing the Game: Innovative Applications of Current Technology

To optimize the degree to which technology can serve as a true force multiplier, the United States must escape the constraints of traditional practices, which often look to technology to automate, and therefore "harden," old ways of doing business. There is no doubt that simple substitution of technology for labor can reduce costs and enable a refocusing of attention to those matters that benefit from human judgment. But these simple substitutions rarely bring order-of-magnitude improvements to the performance of a whole domain.

Based on the preceding four challenges, this section presents four areas in which using currently available technology in new ways can address these hurdles to border control and immigration reform to create a dramatic improvement in performance.

---

[22] Richard M. Stana, "Employment Verification: Agencies Have Improved E-Verify but Significant Challenges Remain," testimony before the Subcommittee on Social Security, House Committee on Ways and Means, April 14, 2011, 6, http://www.gao.gov/assets/130/126065.pdf.
[23] E-Verify queries data held by a variety of agencies but has no control over the accuracy of that data.
[24] Marc R. Rosenblum, "E-Verify: Strengths, Weaknesses, and Proposals for Reform," Migration Policy Institute, February 2011, 6, http://www.migrationpolicy.org/pubs/e-verify-insight.pdf.
[25] Ibid.,13.
[26] Ruth Ellen Wasem, "Unauthorized Aliens' Access to Federal Benefits: Policy and Issues," Congressional Research Service, September 17, 2012, 12, http://www.fas.org/sgp/crs/homesec/RL34500.pdf.

Improving Security at the Physical Border

Richard Falkenrath once called the post-9/11 era the "revolution in border security," in which technological developments have the potential to transform border security.[27] Approaching border security via the lens of how technology can create new, efficient processes offers many potential opportunities for improvement. In recent years, there has been an attempt to implement "virtual fence" technologies along the southern border. The most ambitious of these programs was the Secure Border Initiative Network (SBI*net*), which sought to "cover the entire Southwest border with a highly integrated set of fixed towers"[28] that would enable real-time coordination of sensors to direct surveillance on activity of interest. Unfortunately, the program was plagued by cost overruns, and likely suffered because DHS attempted the project "without many of the in-house program-management, procurement, and technical capabilities to plan, design, build, and implement a cutting-edge system."[29] The lessons from SBI*net* were not that these technologies were wholly ineffective, but that the SBI*net* could not "provide a single technological solution to border security."[30] Rather, proven technologies would have to be tailored to fit the terrain.[31] Many of the technologies DHS sought to harness, including radar, video, and other sensors, will remain important elements of border security.[32] But perhaps the lessons of SBI*net* raise a more important question about whether the notion of 7,500 miles of seamless and impenetrable virtual fence is the most productive way of thinking about the challenge.

Under a reformed view, unmanned aerial vehicles (UAVs) will be important to continued border patrol efforts. UAVs provide much-needed flexibility to deal with a wide array of threats beyond border security, including hurricanes, while eliminating risk to pilots. Further, when UAVs are used as mobile surveillance instruments, CBP can monitor transit zone activity and unguarded sections of the border, all of which will ensure safety and situational awareness.[33] UAVs offer other distinct advantages, including extended ranges and endurance (with the Predator able to fly up to 30 hours), all providing greater capabilities for tracking and prolonged surveillance.[34] Nonetheless, questions remain about the applicability of machines designed for warzones to border security and domestic use. UAVs' limitations include higher operational costs, higher crash rates, and restricted capabilities in bad weather.[35] Further, a 2005 DHS review suggested that due to the extensive logistical support required to operate a single UAV, the cost to operate a UAV exceeded that of manned aerial systems.[36] The report, however, balanced this assessment with the numerous advantages of UAVs and concluded the technology offered significant promise.[37] The relative costs of technology tend to decrease over time as systems advance, become smaller, more capable, and more common—trends that suggest that UAVs may be the future of border security. Currently, CBP has 10 Predator drones, with plans to increase the fleet to 24 by 2016, assuming budget availability.[38] Alternatives, which include miniaturized drones such as those utilized by state and local law enforcement agencies, may be a more economical way to deliver tactical support for agents in the field.

---

[27] Rey Koslowski, "Smart Borders, Virtual Borders or No Borders: Homeland Security Choices for the United States and Canada," *SMU Law Review* (2005): 2, http://www.albany.edu/~rk289758/documents/Koslowski_Smart_Borders_SMU_ law_Review05.pdf.
[28] U.S. Department of Homeland Security, "Report on the Assessment of the Secure Border Initiative-Network (SBI*net*) Program," 1, http://www.globalexchange.org/sites/default/files/DHS_Report.pdf.
[29] Rick "Ozzie" Nelson "The End of SBInet?," CSIS, October 29, 2010, http://csis.org/publication/end-sbinet.
[30] U.S. Department of Homeland Security, "Report on the Assessment of the Secure Border Initiative-Network (SBI*net*) Program," 1.
[31] Ibid.
[32] Demetrios G. Papademetriou and Elizabeth Collett, *A New Architecture for Border Management* (Washington, DC: Migration Policy Institute, March 2011), 10, http://www.migrationpolicy.org/pubs/borderarchitecture.pdf.
[33] Ahern, "Innovative Immigration and Border Control Reform."
[34] Chad C. Haddal and Jeremiah Gertler, "Homeland Security: Unmanned Aerial Vehicles and Border Surveillance," Congressional Research Service, July 8, 2010, 3–4, http://www.fas.org/sgp/crs/homesec/RS21698.pdf.
[35] Ibid., 4.
[36] U.S. Department of Homeland Security, "A Review of Remote Surveillance Technology along U.S. Land Borders," December 2005, 16, http://www.oig.dhs.gov/assets/Mgmt/OIG_06-15_Dec05.pdf.
[37] Ibid.
[38] Gerald Dillingham, "Unmanned Aircraft Systems: Use in the National Airspace System and the Role of the Department of Homeland Security," testimony before the Subcommittee on Oversight, Investigations, and Management, House Committee on Homeland Security, July 19, 2012, 9, http://www.gao.gov/assets/600/592667.pdf.

As evidenced by Israel's struggle to maintain the Gaza blockade against a warren of tunnels,[39] a limited, traditional focus on physical border security may bring diminishing results. Regardless of the general effectiveness of border security technologies and processes, breaches will occur, and legal entrants to the United States will overstay their visas. Accordingly, the U.S. government must apply effective filters within the country to prevent someone who has breached the border or visa conditions from accessing jobs, school, and other benefits. Ultimately, keeping the borders secure involves not only preventing undesirable or ineligible individuals from entering, but also allowing those with legitimate interests to enter, and ensuring that non-citizens who have been granted entry comply with the conditions of their visa. In contrast to the SBI*net* vision of a virtual fence for the physical border, perhaps the "interior compliance" answer to border control is a challenge to be achieved through better use of cyberspace. This is an approach that requires reliable ways to verify an individual's identity.

Improving Identity Management

Indeed, applicant identification and verification is relevant to every challenge mentioned above. Identity is the common link that connects visa applications, advance passenger manifests, port-of-entry screening, overstay monitoring, employment eligibility, and access to the rights and benefits that make it possible to have an economic life in the United States. It is the core mechanism by which undesirable or ineligible individuals are prevented from crossing the border, and accessing those privileges. However, "[t]he use of fraudulent identities is a continual weakness with respect to both immigration control and counterterrorism systems."[40] One key question is how to improve the integrity of the identity information gathered, and connect that information consistently to the physical person with whom it is associated.

One possible solution is expanding the use of biometrics in identification to counter identity fraud. Broad utilization of biometric identities could improve the integrity of internal enforcement mechanisms like E-Verify, SAVE, Student and Exchange Visitor Information System (SEVIS), and Exit for visa compliance. One of the major challenges is how to implement biometric screening points on a broader scale in an efficient and effective way, without veering into the politically charged national identity debate.[41] Here is an example where technologies that have become consumerized over the past decade provide a new way of using biometric identification. Mobile phones and tablets have become ubiquitous. Combining these devices with a focus on the needs of the individual presents an opportunity to revolutionize identification in ways that enhance privacy.

One important improvement would be to minimize the broad overlap and redundancy that currently exists with respect to identification activities. Multiple agencies, and at times even subagencies, collect and manage the same identifying information from applicants. Many require usernames and passwords to access electronic services. These repetitive practices are expensive for the government, and often stray beyond the agency's core mission. Likewise, such practices place burdens upon applicants who have to reprove who they are with each application, and keep track of numerous, infrequently used passwords. An effort to consolidate these activities by the private sector on behalf of the individual, or at least offer a single portal that allows an individual to manage all iterations of their identity throughout government databases,[42] could lower government costs and improve data accuracy. But it is essential that such an initiative strengthens requirements to ensure the uniqueness of identity claims, examine the evidence underlying biographic claims, and secure the individual's connection (authentications) with this data.

Such efforts are part of a market that is emerging to conduct government and business transactions in a new way. As envisioned by the principles of the National Strategy for Trusted Identities in Cyberspace (NSTIC), individuals should be able to establish their trusted identity one time and reuse it with government and commercial relying parties. NSTIC "envisions a cyber-world—the Identity Ecosystem" that allows "people to choose among multiple identity providers—

[39] See, for example, Yue Wang, "It Takes a Smuggler to Satisfy KFC Cravings in Gaza," *Time*, May 17, 2013, http://newsfeed.time.com/2013/05/17/it-takes-a-smuggler-to-satisfy-kfc-cravings-in-gaza/.
[40] Papademetriou and Collett, *A New Architecture*, 6.
[41] This debate over a national identification card is rife with political, national security, and privacy sensitivities. Extensive further study, discussion, and consideration of costs, benefits, and options is necessary, and this paper neither advocates for nor rejects the concept; rather, it simply highlights the issue set as a particularly complex subject within the context of border and immigration reform.
[42] The obvious exception relates to classified or law-enforcement records.

both private and public—that would issue trusted credentials that prove identity."[43] The NSTIC model envisions replacing stove-piped usernames and passwords with more secure forms of digital credentials that can be reused by the individual across venues and platforms, in privacy-preserving ways. Ideally, this initiative would simplify the process of managing identities, strengthen authentication, and limit opportunities for fraud or the potential for errors in identity verification processes. The technologies to enable this vision already exist, and need only be configured for the purposes of immigration and border control. Such efforts could provide ways to unify identities belonging to the same individual across multiple platforms, and facilitate the flow of information between multiple sources to ensure that when needed, a complete understanding of the individual's engagement with the enterprise is available.

Modern mobile technologies and services are a key component of the emerging identity ecosystem. Smart phones enable multifactor authentication, combining "something you have" with "something you know"; offer a platform for biometric sensors to add "something you are"[44]; facilitate the use of text-messaged one-time passcodes as secondary verification tools; and introduce geolocation as a verification data-point. The integration of smartphones and emerging authentication approaches offers the prospect that the technologies of authentication can be integrated into a tool that individuals use every day. Most importantly, consumerized mobile technologies offer the very real possibility of changing the traditional dynamic of identification from something that is controlled by the enterprises individuals engage with, to being something that individuals control. This increases privacy for the individual.

Leveraging these mobile technologies within an NSTIC-like framework would make identification more convenient, cost-efficient, secure, and privacy-preserving for individuals by minimizing the bureaucracy around it. The results would include stronger integrity across the visa, border, and immigration system, enabled by a series of virtual checkpoints that seamlessly reserve access to rights, entitlements, and benefits for their rightful beneficiaries. In this way, cyberspace offers the opportunity to complement initiatives that push the border off-shore with mechanisms that allow border control to be brought into the heart of the economy.

Mobile technologies also broaden access. For example, small businesses that would be hard-pressed to install and maintain dedicated biometric technologies could leverage their employees' smartphones and mobile applications to verify identities and ensure compliance with employment laws. Such mechanisms could be used to verify identity in automated border-control environments, as well as in transactions with government systems such as SAVE and SEVIS. They could be used in airline check-in operations, and by foreign partners, to enable biometric exit reporting. This process will still require the development of some new platforms that simplify the connection of consumer infrastructure with enterprise infrastructure, but framed within commercially developed identity service solutions, consumerized mobile technology offers both the promise of being less infrastructure-hungry than traditional single-purpose technology solutions (e.g., US-VISIT), and of leveraging widely available public infrastructure (wireless networks, the internet) for new purposes. DHS's struggle to implement a land border-exit system provides one example of the problems with a 'big' system approach. The process of development, design, construction, and implementation of a traditionally conceived exit solution is not only difficult, but costly.[45] Adapting available and emerging technologies within new business practices for identification can eliminate expensive research, design, and construction elements, lower the barriers to entry for individuals and small businesses, and accelerate implementation.

Making Full Use of Cyberspace to Share Information

Access to information about specific individuals across multiple agencies requires the ability, and willingness, of information-collecting organizations to cooperate and share their data. Since 9/11, the United States and its international security partners have made significant progress in this area.

The strategic importance of information sharing is undisputed, but data inaccuracies and inconsistencies between multiple databases continue to enable illegal activity and hamper law-abiding individuals. With proper execution, it could be

[43] National Strategy for Trusted Identities in Cyberspace, "Making Online Transactions Safer, Faster, and More Private," http://www.nist.gov/nstic/.
[44] Tarun Wadhwa, "Your Next Phone Is Likely to Include Fingerprint, Facial, and Voice Recognition," *Forbes*, March 29, 2013, http://www.forbes.com/sites/tarunwadhwa/2013/03/29/why-your-next-phone-will-include-fingerprint-facial-and-voice-recognition/.
[45] Stana, "Visa Security."

possible to ensure the consistency of identifying data across government agencies, and prevent fraud by eliminating the ability of individuals to create multiple legal identities. Further, being able to connect existing information in shared databases—for example, those shared between the FBI and CBP—can enable the interdiction of suspects at the borders. A good example of such cooperative efforts is the interoperability of DHS's Automated Biometric Identification System (IDENT), which uses biometric records obtained through the US-VISIT program, and the FBI's Integrated Automated Fingerprint Identification System (IAFIS), which share data and facilitate cross-referencing.[46] The success of these systems comes down to the ability to search for matches based on biometrics. Similarly, the Student and Exchange Visitor Information System (SEVIS) "interfaces with a number of law enforcement and intelligence databases, including IDENT and the Foreign Terrorist Tracking Task Force."[47] In the same vein, the Verification Information System (VIS) that provides the platform for E-Verify and SAVE functions as a query service against multiple, disparate federal and state databases. Its performance is limited only by the quality of information in those downstream systems, something over which VIS has no control. This ability to access information across agencies and databases improves the ability of enforcement agencies to assess threats and work cooperatively to address them. Only by interconnecting databases and sharing information can these data be cross-matched and analyzed.

Information sharing is important at all levels of the border and immigration process, from preventing visa overstays, to intercepting threats, to limiting the expenditure of scarce resources on collecting the same information multiple times by multiple parties. Working with trusted partner countries is also an important element in border control and immigration innovations. With governments placing "greater emphasis on collecting data on international travelers before they arrive at the border," such partnerships can be essential for interdicting individuals with malicious intent.[48] Such cooperative efforts to date, however, have been limited to mostly simple border-control efforts. For example, while the European Union "allows Member states to use API [Advanced Passenger Information] data, only a handful have enacted legislation to take advantage of this information source."[49] By contrast, the United States identified API as a key asset following 9/11 and embraced it as part of the border-screening process.[50] Sharing between the United States and the European Union has been cumbersome and contentious, with negotiations stretching from 2004 to 2012's "Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security."[51] The European Union has been effective with internal information-sharing mechanisms, however, such as the Schengen Information System and the Visa Information System, which provide Schengen participant countries updated, accurate data on entries to the Schengen area.[52] Given these challenges, it is important that consideration be given for modern technology to enable new practices of information sharing.

The user-centric identity service approach discussed above offers such an opportunity. To effectively share information, the commercial entities and government agencies involved in facilitating border crossing must have access to consistent, verified identifying information, accompanied by a level of confidence that an identity is unique.

One way of addressing the historical challenges—related to concerns about both individual privacy and rules governing the information transfer between and among jurisdictions—in this area would be to request and receive consent from individual travelers, allowing national officials to share data across particular borders. This sort of solution would require countries, on a bilateral or multilateral basis, to agree on shared standards for commercial identity services, standards that

---

[46] Michelle Mittlestadt, Burke Speaker, Doris Meissner, and Muzaffar Chishti, "Through the Prism of National Security: Major Immigration Policy and Program Changes in the Decade Since 9/11," Migration Policy Institute, August 2011, 5–6, http://www.migrationpolicy.org/pubs/fs23_post-9-11policy.pdf.
[47] Ibid., 6.
[48] Elizabeth Collett, *Emerging Transatlantic Security Dilemmas in Border Management* (Washington, DC: Migration Policy Institute, June 2011), 3, http://www.migrationpolicy.org/pubs/securitydilemmas-2011.pdf.
[49] Papademetriou and Collett, *A New Architecture*, 5.
[50] Ibid., 4.
[51] "Agreement between the United States of American and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security," *Official Journal of the European Union,* November 8, 2012, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:215:0005:0014:EN:PDF.
[52] Collett, *Emerging Transatlantic Security Dilemmas*, 3.

take into account privacy concerns.[53] Such an arrangement would also likely require the broad implementation of an NSTIC-like identity solution that provides individuals with trustworthy authentication capabilities.

Improving the Use of Scarce Resources

Technology, when used strategically, can act as a force multiplier. Current budget constraints make the potential benefits of technological innovation more important than ever. Adopting technology for new ways of doing business should thus be seen not only as a way to make border control and immigration processes faster, more efficient, and more accurate, but also less economically burdensome. In particular, intelligent use of technology within new business practices would allow human resources to reallocate their time from low-value work that can be automated, toward a stronger focus on activities that require human judgment, like intelligence collection, situational assessments, and apprehension. Intelligent automation will also reduce the effort and cost of assessing the compliance of legitimate travelers.

Further, expanding trusted- and frequent-traveler programs can facilitate faster, friendlier border crossing, and airport security. Automation-assisted means, such as kiosks or e-gates, can process travelers in ways that reduce and eliminate wait times and allow scarce human resources to be focused on riskier travelers. That said, kiosks and bilateral systems can become expensive to operate on a large scale. As such, supplementing the use of kiosks with travelers' own mobile devices can exponentially expand the benefit while limiting costs. "Bring Your Own Identity" approaches that operate within an approved trust framework that connects enrollment, identity assurance, and authentication services could be leveraged to step up electronic authentication to "level 3" and "level 4" confidence,[54] while achieving the same experience of personalization and convenience consumers increasingly expect in retail environments.[55]

Establishing a standardized identity ecosystem that promotes interoperability across the public and private sectors could improve cost-effectiveness by helping to facilitate the creation of a trusted identity for each individual in every unique credential context, eliminate the secondary costs of identity theft, and preclude the implementation of multiple redundant programs. In additional, border processes could use innovative technological solutions to identify *known* travelers (i.e., with trusted identities) from *unknown* travelers, which could occur even before verifying an individual's citizenship status and determining whether an individual has a right to enter the country or access benefits, rights, and privileges. Such identity solutions could help to create high-confidence connections between separate accounts and records in various databases, when and as appropriate and authorized.

Finally, reinventing the business process with available technology offers the possibility of simplifying and personalizing visa and citizenship processes. Trusted identity solutions can enable individuals to securely engage with relevant agencies through their home computers, tablets, or mobile phones. This, in turn, enables the development of user-friendly interface experiences that include tutorial-type programs that walk individuals through each stage of application with graphics and video instead of text-based explanations. Video conferencing is now within reach of anyone with a Google or Skype account, something that could be leveraged for interviews. Such solutions will help applicants quickly and accurately complete their applications to facilitate acceptance into a program of interest. This additional efficiency up front can improve downstream performance by eliminating data errors that arise through transcription from paper to electronic systems, and thereby reduce processing, wait times, and costs. Indeed, one of the core advantages of technology is its potential to make the most of limited resources. Increases in value and efficiency—and enhancing the experience of engaging with the agency—should be a core mission of any border control and immigration innovation effort.

Conclusion

Governments are often late adopters of new technologies—they tend to use technology to facilitate yesterday's way of doing business. Institutions can be slow to change and adjustments can be expensive. Infrastructure requirements often complicate the implementation of new technology. Currently, there are marked gaps among the operational possibilities

[53] It should be noted that the pursuit of such agreed-upon bilateral or multilateral standards would not prevent an individual government from determining expectations for commercial identity solution or from using such solutions within its own borders.
[54] For definitions of authentication standards, see Shirley Radack, "Electronic Authentication: Guidance for Selecting Secure Techniques," *iTL Bulletin*, August 2004, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=150430.
[55] For a short video on how this works, see Bank2Book, "Starbucks Mobile Payment Live Demonstration," YouTube, January 27, 2011, http://www.youtube.com/watch?v=or6U0GeZ4j0.

enabled by today's technological advances, an appreciation of the possibilities they can create, and their implementation by immigration and border control mechanisms. By being open to new ways of doing business, border and immigration agencies could leverage these new technologies in ways that dramatically improve their ability to perform. New methods for data collection and analysis, remote surveillance, and the use of biometric identifiers all have the potential to revolutionize ways in which the United States secures its borders and cooperates across agencies and nations. User-centric identification practices, combined with increasingly ubiquitous mobile technologies, provide the foundation for exciting new ways of getting the job done. If done right, applied technological innovation can help us invent effective, efficient, accurate, and budget-friendly border and immigration processes suitable to the twenty-first century.

Technology, however, is simply a tool. It brings little value unless it is integrated into a broad and comprehensive reform and innovation program that leverages the knowledge and capabilities of a wide range of sources, including the private sector. For example, border control and immigration might benefit from a concerted effort to reform its "business model." Every organization has a value chain—that is, the unique collection of goods, raw materials, and activities that go into the creation of a final product or outcome. In the private sector, organizations that are able to efficiently and profitably link those items together produce better value, and gain a competitive advantage. Government agencies do not face the constraints or pressure of competition. There remains an imperative to find innovative ways for each agency to deliver its outcomes efficiently and effectively, while eliminating duplicative activities better suited to other parties. For visa, border, and immigration agencies, these outcomes—such as border integrity—are unique, abstract, and difficult to measure. Nevertheless, lessons abound in the increasingly intangible service-driven economy of the United States. Such knowledge can be leveraged through public/private partnerships that build on the relative strengths of each sector.

Innovation and reform efforts are fraught with challenges and ripe with opportunities. Perhaps the most significant are the concerns about privacy, which color the debate on many of the current technologies. However, the technologies to simultaneously enhance privacy, security, and border performance exist, and are increasingly powerful and affordable. Border control and immigration must not only keep pace with the continual evolution of technology, but must reinvent themselves when technologies create opportunities to dramatically enhance agencies' ability to achieve their business and mission objectives. Only by updating and innovating today can the U.S. government address the challenges and threats of tomorrow.

Stephanie Sanok Kostro *is acting director of the Homeland Security and Counterterrorism Program and deputy director of the International Security Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.* ***Scott F. Mann*** *is a research associate with the CSIS Harold Brown Chair in Defense Policy Studies.*