

BIG DATA AT THE BORDER:
BALANCING VISA-FREE TRAVEL AND SECURITY IN A DIGITAL AGE

Nathan Alexander Sales
Syracuse University College of Law

ABSTRACT

The United States and other developed nations increasingly are replacing their traditional, visa-based systems for regulating international travel with new regimes that combine visa-free travel with computer systems that analyze large troves of data in an attempt to identify risky travelers. While this shift has helped facilitate trade, tourism, and global interconnectivity, and offers important national-security benefits, the data collection on which it relies raises important questions about privacy and civil liberties.

INTRODUCTION

It has never been easier to cross international borders. In recent decades, a number of industrialized nations have implemented new, visa-free approaches to international travel: the Visa Waiver Program (VWP) in the United States, the Schengen Area in Europe, and so on. Yet standing alongside these permissive regimes—especially in the U.S. but increasingly in other countries as well—is the expanding governmental collection and analysis of large troves of potentially sensitive information about inbound travelers. These two trends are not isolated developments but rather operate together as an entirely new system for regulating international travel.

This short paper—which is informed by my prior service at the U.S. Department of Justice and Department of Homeland Security, and which builds on previous work on data analysis and national security¹—discusses this new approach and its legal and policy implications. The paper begins by describing the two elements that comprise the emerging visa-free, data-centric regime as it is implemented in the United States: the VWP, which allows citizens of certain countries to travel to the U.S. without a visa, and the Automated Targeting System (ATS), which collects and analyzes airline reservation data to identify potentially risky travelers. The paper concludes with some observations on some of the costs and benefits of this new regime. In sum, the combination of no-visa travel and data analysis produces substantial economic, cultural, and national-security gains. Although this new regime relies on government access to large volumes of passenger data, it paradoxically has the potential to preserve individual privacy more effectively than the visa-based system it replaces.

¹ Nathan Alexander Sales, *Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy*, 10 ISJLP 523 (2014); Stewart A. Baker & Nathan Alexander Sales, *Homeland Security, Information Policy, and the Transatlantic Alliance*, in *LEGAL ISSUES IN THE STRUGGLE AGAINST TERROR* 277 (John Norton Moore & Robert F. Turner eds.; Carolina Academic Press; 2010).

I. VISA-FREE TRAVEL

Congress established the Visa Waiver Program in 1986 to facilitate travel between the United States and its closest allies. The program allows citizens from member countries to travel to the U.S. for business or tourism for up to 90 days without first obtaining a visa.² There is no longer any need to complete detailed visa application forms, compile bank statements and other supporting documentation, travel considerable distances to cities housing U.S. diplomatic missions, and undergo time-consuming interviews with consular officials. VWP travelers can simply book a flight and hop on a plane.

The United Kingdom was the first country to join the program in July 1988; Japan followed a few months later. Through the mid-2000s, the VWP was primarily a club for the wealthy, industrialized democracies of Western Europe—members included Belgium, France, Germany, Italy, the Netherlands, Spain, and Switzerland, along with a handful of other prosperous countries elsewhere in the world like Australia and New Zealand. After the end of the Cold War and coinciding with the eastward expansion of NATO and the EU, Congress enacted legislation in 2007 that enabled a number of nations from Central and Eastern Europe to join the VWP—the Czech Republic, Estonia, Hungary, Latvia, Lithuania, and Slovakia—as well as Malta and South Korea. The most recent additions are Taiwan (2012) and Chile (2014). In all, 38 countries are now members of the program.³

The VWP can be thought of as a junior-varsity version of Europe’s Schengen Agreement, conceived around the same time. Schengen, which was signed in 1985 and implemented beginning a decade later, abolishes internal border controls among signatory nations. Whereas the more ambitious Schengen Agreement allows the citizens of member countries to travel within Europe without a passport, the VWP more modestly leaves border controls in place but expedites the process of clearing them. In short, Schengen eliminates the need for a passport while the VWP eliminates the need for a visa.

To be admitted to the VWP, countries must meet a number of statutory criteria.⁴ Among other requirements, they must extend reciprocal visa-free travel to American citizens, issue machine-readable passports, and so on. Traditionally, the most important factor bearing on a country’s eligibility for the program was that its citizens posed a low risk of illegal economic migration—i.e., overstaying the terms of their admission in search of work. To address this risk, the VWP statute required candidate countries to have a visa refusal rate—which is the sum of consular officials’ predictions that applicants from a particular country would overstay in the U.S.—lower than 3 percent.⁵

² See 8 U.S.C. § 1187(a).

³ <http://www.dhs.gov/visa-waiver-program-requirements>.

⁴ See 8 U.S.C. § 1187(a)(2)(A), (c)(2).

⁵ See *id.* § 1187(c)(2)(A)(ii).

The 2007 legislation referenced above made two major changes to this scheme. First, Congress temporarily suspended the requirement of a 3 percent visa refusal rate, creating a window for countries with rates as high as 10 percent to join the program.⁶ (This is what enabled certain countries from Central and Eastern Europe to become members.) Second, Congress called for more information sharing among the program's participants. Shifting from visa-based to visa-free travel deprives the government of certain information about visitors. WWP travelers no longer need to complete detailed visa applications, provide supporting documentation (such as bank statements or pay stubs), or participate in interviews with consular officials—all of which are lost opportunities to spot risky travelers. The revised VWP compensates for this information loss with alternative sources of data that can be used to screen for threats.

For instance, the 2007 legislation requires member countries to inform the United States about lost and stolen passports, reducing the risk that terrorists and criminals might travel on forged documents.⁷ Members must enter reciprocal agreements with the U.S. to exchange watchlists of known and suspected terrorists—the Homeland Security Presidential Directive 6 (HSPD-6) agreements.⁸ They also must agree to mutually share criminal history information, including biometric data like fingerprints and DNA—the so-called Preventing and Combating Serious Crime (PCSC) agreements.⁹ The 2007 law further requires individual VWP travelers to provide basic biographic information, such as names and passport numbers, through an online form called the Electronic System for Travel Authorization (ESTA).¹⁰ (ESTA is based on a similar program pioneered by Australia known as the Electronic Travel Authorization, or ETA.) And as described in the next section, a separate statute directs airlines to turn over reservation data for all U.S.-bound passengers, including from visa waiver countries.¹¹ These information-sharing measures enable authorities to screen inbound passengers to determine which pose a greater risk of terrorism or criminal activity and therefore merit extra scrutiny at the border.

II. AIRLINE RESERVATION DATA

With the rise of visa-free travel, and the resulting loss of consular interviews and other advance information about inbound travelers, government officials have found it necessary to develop substitute sources of traveler data. In particular, U.S. counterterrorism officials have come to rely heavily on airline reservation data—known as passenger name records, or PNR—to screen for terrorists and other potentially risky travelers. Terrorism and travel are inextricably linked. Consider the steps that often must be undertaken to accomplish a terrorist attack. The operative must be trained; he must receive funding; he must meet with his handlers to receive direction; he must enter the country he means to strike; and he must case his intended targets. Each of those steps typically involves travel. For that reason, the 9/11 Commission emphasized that a terrorist's

⁶ *See id.* § 1187(c)(8)(B)(v)(I).

⁷ *See id.* § 1187(c)(2)(D).

⁸ *See id.* § 1187(c)(2)(F).

⁹ *See id.*

¹⁰ *See id.* § 1187(a)(11).

¹¹ *See* 49 U.S.C. § 44909(c).

ability to travel is “as important as weapons.”¹² It therefore called on the government to deploy “[i]nformation systems able to . . . detect potential terrorist indicators . . . at consulates, at primary border inspection lines, in immigration services offices, and in intelligence and enforcement units.”¹³

PNR consists of the basic personal information that travelers provide to airlines or travel agents in the course of booking airline reservations. It typically includes anodyne information such as name, passport number, frequent flyer number, address, telephone number, and so on. This data may be fairly simple, but it can be a powerful analytical resource. At the most basic level, passenger data enables officials to check travelers’ names against lists of known or suspected terrorists.¹⁴ Of course, watchlisting is not without its downsides. The technique might ensnare innocent travelers, and it is incapable of detecting unknown threats. Which is why the more sophisticated analytics made possible by PNR are especially important. By using simple forms of link analysis or contact chaining, PNR makes it possible to discover hidden connections between known terrorists and their previously unknown associates. If a traveler has used the same phone number or mailing address as Khalid Shaikh Mohammed, the mastermind of the September 11 plot, he probably merits a closer look than a typical airline passenger.

The computer system the U.S. government uses to analyze airline reservation data is known as the Automated Targeting System. ATS was first developed in the 1980s to assist the Customs Service in screening inbound cargo for illegal narcotics, counterfeit goods, and other contraband. After 9/11, the system’s capabilities were enhanced to enable the screening of inbound passengers. Today, the government uses ATS—and the airline reservation data on which the system relies—to help determine which of the 87 million passengers who enter the United States by air each year might pose a greater risk and therefore should be subject to a little extra scrutiny.¹⁵

The legal authorities under which this information is collected and analyzed are fairly straightforward. Less than two months after the 9/11 attacks, Congress enacted the Aviation and Transportation Security Act of 2001. Section 115 of that legislation directs all air carriers that fly to the United States to provide the government with a passenger and crew manifest (including each passenger and crew member’s full name, their dates of birth, their passport numbers, and “[s]uch other information” as is deemed “reasonably necessary to ensure aviation safety”). It also specifically requires airlines to turn over “passenger name record information.”¹⁶

As for the Constitution, the Fourth Amendment’s prohibition on unreasonable searches and seizures generally requires the government to obtain a search warrant upon a showing of probable cause before accessing information in which the holder has a “reasonable expectation of

¹² Nat’l Comm’n on Terrorist Attacks Upon the U.S., The 9/11 Commission Report 384 (2004).

¹³ *Id.* at 385.

¹⁴ See *id.*

¹⁵ See U.S. Customs and Border Protection, Automated Targeting System, System of Records, 72 Fed. Reg. 43,650, 43,651 (Aug. 6, 2007).

¹⁶ 49 U.S.C. § 44909(c)(2), (3).

privacy.”¹⁷ Over the course of several decades, the Supreme Court has held that a person generally has no such reasonable expectation in data he turns over to a third party in the ordinary course of business. For example, the government need not obtain a search warrant before installing a pen register or trap and trace device—which collect data about the numbers dialed or received by a particular telephone, but not the content of the conversations themselves—because the caller necessarily reveals that information to the phone company when he places a call.¹⁸ Nor is a warrant needed when the government asks a bank to turn over a customer’s financial records. Because a “depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government,” a depositor has no “legitimate ‘expectation of privacy’ in . . . information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.”¹⁹

Of course, the “third party doctrine,” as it is known, has come in for its fair share of criticism. The leading criminal law treatise in the United States pronounces it “dead wrong”²⁰ and one member of the Supreme Court recently called for its reconsideration.²¹ Whatever the strengths or weaknesses of the doctrine, however, PNR is a fairly straightforward application of it. As is true with phone numbers and financial information, travelers provide basic personal data to airlines or travel agents in the ordinary course of booking a reservation—the name they wish to appear on the ticket, the method of payment, a phone number at which they can be contacted in the event there is a schedule change, and so on. Airline reservation data thus fits pretty comfortably within established constitutional norms on government access to information that has been conveyed to third parties.

As for international law, the leading treaty applicable to passenger screening is the 1944 Chicago Convention on International Civil Aviation. The convention acknowledges that every nation has “complete and exclusive sovereignty” over its airspace.²² As a corollary, Article 11 expressly directs airlines to comply with a country’s laws “relating to the admission to or departure from its territory of aircraft engaged in international air navigation.”²³ (A similar obligation attaches to individual passengers.²⁴) As we’ve seen, one of those laws with which U.S.-bound airlines must comply is the obligation to share PNR and other passenger information. The

¹⁷ *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

¹⁸ *See Smith v. Maryland*, 442 U.S. 735, 744 (1979) (“When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and ‘exposed’ that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.”).

¹⁹ *United States v. Miller*, 425 U.S. 435, 442, 443 (1976); *see also id.* at 443 (“[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.”).

²⁰ 1 Wayne R. LaFare, *Search and Seizure: A Treatise on the Fourth Amendment* § 2.7 (4th ed. 2004).

²¹ *See United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

²² Chicago Convention on International Civil Aviation art.1, Dec. 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295.

²³ *Id.* art. 11.

²⁴ *Id.* art. 13.

government then uses the data for the various purposes spelled out in the Convention—e.g., deciding whether a particular traveler should be allowed to enter the country, assessing his immigration status, checking the authenticity of his passport, and so on. Indeed, the Convention expressly requires airlines to collect and turn over basic information about the passengers they carry. “Every aircraft” that flies internationally is directed to carry “a list of [passengers’] names and places of embarkation and destination”²⁵ and to make that list available to authorities upon arrival.²⁶ That’s an embryonic form of PNR.

Passenger reservation data is a centerpiece of U.S. immigration, customs, and counterterrorism efforts at the border, but it has proven enduringly controversial with some lawmakers in Europe.²⁷ Since 2004, U.S. and EU officials have negotiated a series of agreements that impose various restrictions on the United States’s collection and use of European PNR. Nevertheless, as with the similarities between the VWP and the Schengen Zone, a transatlantic convergence might be possible here as well. There are some indications that Europe may now be on the verge of developing a PNR system of its own, in the wake of the *Charlie Hebdo* attacks in early 2015.²⁸

III. COSTS AND BENEFITS

The two trends I’ve sketched above—the rise of visa-free travel and the emergence of data-based systems for screening travelers—are not isolated developments but together combine to create an entirely new regime for regulating the movement of people across international borders. Unlike a traditional visa-based system, which relies on detailed questionnaires and in-person consular interviews to determine a person’s eligibility to travel, the emerging data-centric regime assesses traveler suitability primarily by analyzing large volumes of a narrow range of personal information—namely, airline reservation data. This concluding section describes some of the costs and benefits of this emerging regime. The economic and social benefits of visa-free travel are fairly obvious. And despite the fact that this new system depends on the collection and analysis of huge troves of passenger data, the emerging regime somewhat counterintuitively actually can be beneficial for individual privacy—or at least certain aspects of individual privacy.

By any measure, visa-free travel has been a resounding success. The abolition of the visa requirement for travel between the United States and its closest allies has made it considerably easier to cross international borders. Tourists and business travelers no longer need to complete detailed visa applications, assemble bank statements and other supporting documentation, travel perhaps considerable distances to the nearest city with a consular post, wait in line at the consulate, submit to an interview, and then wait months to hear if their applications have been granted or denied. They can simply book a flight and get on a plane. During an official visit to Seoul in the mid-2000s, my South Korean counterpart pointed out the long queue of people outside the U.S. embassy waiting to present their visa applications to American consular officials. Not only was

²⁵ *Id.* art. 29.

²⁶ *Id.* art. 16.

²⁷ See Baker & Sales, *supra* note 1.

²⁸ See, e.g., Michael Birnbaum, After Paris Attacks, E.U. Leaders Call for More Sharing of Information, Intelligence, WASH. POST, Jan. 19, 2015.

this an irritant in the bilateral relationship between our two countries, he said, it was an enormous inconvenience for the South Korean citizens who had to take a substantial amount of time out of their busy lives to obtain permission to visit friends or family, go on vacation, or attend business meetings in the U.S. With the expansion of visa-free travel, those queues increasingly are becoming a historical relic. That isn't just beneficial for foreign citizens who wish to visit the United States; American travelers benefit too, as one of the conditions of VWP membership is that the candidate country must grant reciprocal visa-free travel to U.S. citizens.²⁹

Visa-free travel is more than just convenient for individual travelers, it also produces important benefits for society as a whole. The VWP vastly increases the amount of travel to the United States. In 2012, 19.1 million people entered the U.S. under the program, up from about 15 million in 2007 (the year before the program's substantial expansion in 2008).³⁰ One recent academic study estimated that the VWP results in an additional 1.8 million to 2.7 million tourist/business trips from member countries each year.³¹ Indeed, the program was responsible for some 45 percent of all tourists and business travelers who entered the United States in 2010.³²

These visitors spend considerable sums of money while in the U.S. A Government Accountability Office (GAO) report from the previous decade found that, "in 2000, travelers from visa waiver countries spent an estimated \$39.6 billion in the United States, accounting for 57 percent of overseas tourist spending."³³ That spending has multiplier effects, as "every dollar spent directly by a traveler in the United States translates into \$1.89 to \$2.33 for the U.S. economy."³⁴ In all, according to the GAO, "visa waiver travelers' direct and indirect spending within the United States added between \$75 billion and \$102 billion to the U.S. gross domestic product in 2000."³⁵

The combination of visa free travel and data analysis also reduces administrative costs. Because VWP travelers no longer must participate in consular interviews before traveling, the State Department is able to substantially reduce the size of its corps of officers at diplomatic posts overseas. The resulting savings are significant. The GAO has indicated that, if the VWP did not exist, "we estimate that the department's initial costs to process the additional workload would likely range between \$739 million and \$1.28 billion and that annual recurring costs would likely range between \$522 million and \$810 million."³⁶ (Of course, some of these savings are offset by the additional expenses associated with using the ATS to collect and analyze passenger reservation

²⁹ 8 U.S.C. § 1187(a)(2)(A).

³⁰ Congressional Research Service, *Visa Waiver Program* 8-9 (2014).

³¹ Xiaochu Hu, Economic Benefits Associated with the Visa Waiver Program—A Difference-in-Difference Approach, 7 GLOBAL J. BUS. RESEARCH 81, 88 (2013).

³² *Id.* at 81.

³³ Gov't Accountability Office, *Border Security: Implications of Eliminating the Visa Waiver Program* 22 (2002).

³⁴ *Id.*

³⁵ *Id.*

³⁶ *Id.* at 23.

data, but it seems unlikely that these costs are anywhere near the costs of fully staffed consular offices in the 38 VWP member countries.)

In addition to these economic gains, data analysis offers important national-security benefits. Using the technique of contact chaining, analysts can use passenger reservation data to identify the hidden connections between known terrorists and their unknown associates. According to a Markle Foundation report, if counterterrorism investigators had been able before 9/11 to apply rudimentary link analysis techniques to airline reservation data and related information, they could have uncovered the ties among all 19 of the al Qaeda hijackers. Start with two men who helped fly American Airlines flight 77 into the Pentagon: Nawaq Alhamzi and Khalid Al-Midhar. Their names appeared on a U.S. watchlist, because they previously had been spotted at a terrorist meeting in Malaysia. So they would have been flagged when they bought their tickets. Tugging on that thread would have revealed three other hijackers who used the same addresses as the first two: Salem Al-Hamzi, Marwan Al-Shehhi, and Mohamed Atta, the plot's operational ringleader. Officials would have discovered another hijacker (Majed Moqed) who used the same frequent-flyer number as Al-Midhar. Five other hijackers used the same phone numbers as Mohamed Atta: Fayez Ahmed, Mohand Alshehri, Wail Alshehri, Waleed Alshehri, and Abdulaziz Alomari. That's eleven of 19. Officials could have found a twelfth hijacker in an INS watch list for expired visas (Ahmed Alghamdi), and the remaining seven could have been flagged through him by matching other basic information.³⁷

Airline reservation data is good for more than Monday morning quarterbacking; it has also produced a number of operational successes. For instance, in 2003, a Jordanian named Ra'ed al-Banna landed in Chicago after a long international flight. His paperwork was in perfect order: He held a legitimate passport, he had obtained a visa authorizing him to work in the United States, and he had previously visited the U.S. without incident. Nevertheless, he had been flagged by ATS as someone who deserved a little extra scrutiny. The officers who questioned him found him evasive, so they refused him entry, took his fingerprints, and put him on the next flight home. A year and a half later, a massive car bomb detonated in Hilla, Iraq, killing 132 police recruits. "The driver was Ra'ed al-Banna. We know that because when authorities found the steering wheel of his car, his forearm was still chained to it."³⁸ It's impossible to know whether al-Banna intended to carry out a similar attack in the United States. But we're fortunate not to have found out.

Similarly, in 2006, at Minneapolis-St. Paul airport, DHS officials used airline reservation data and other information to flag a risky traveler for additional scrutiny before he arrived. Once the passenger was referred to secondary inspection, it was discovered that he had a manual on how to make Improvised Explosive Devices, or "IEDs"—the kind of bombs used to kill and maim allied forces in Afghanistan and Iraq. Inspecting the traveler's computer, officers also found video clips of IEDs being used to kill soldiers and destroy vehicles, as well as a video on martyrdom. The passenger later pled guilty to visa fraud.³⁹

³⁷ Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force 28 (2002).

³⁸ Baker & Sales, *supra* note 1, at 278,

³⁹ See Remarks of Stewart Baker, Assistant Sec'y for Policy, Dep't of Homeland Security, at the Ctr. for Strategic and Int'l Studies (Dec. 19, 2006), http://www.dhs.gov/xnews/speeches/sp_1166557969765.shtm.

Data analysis also enables the government to resolve potential false positives more quickly—which is beneficial both for national-security officials and for individual travelers. Suppose the name “U. Abdulmutallab” appears on the no-fly list, and a passenger with the same name is traveling from Amsterdam to Detroit. If the only thing officials know about the passenger is his name, he likely is going to be pulled aside at Schiphol and asked a number of questions to establish his true identity. Making more information available to the government allows that process of identity resolution to take place behind the scenes, and more quickly. If officials have not just U. Abdulmutallab’s name, but also his date of birth, his passport number, and so on, it becomes possible to know immediately whether this is a man to worry about or an innocent with the misfortune of sharing a name with an international terrorist.

The economic and national-security implications of visa-free travel are fairly obvious, but the emerging data-centric regime also has important consequences for privacy and civil liberties. Many observers, both in the United States and abroad, have raised privacy concerns about the government’s collection and analysis of huge troves of passenger data. In the early 2000s, these worries led the U.S. Congress to enact legislation that essentially barred the government from deploying the so-called CAPPs II system, which would have used airline reservations and other commercial data to screen passengers on domestic flights. (The law did not restrict the government from screening passengers on *international* flights, which remains lawful.) In a similar way, a number of EU policymakers have raised concerns about the U.S. government’s access to European passenger reservation data and have sought to negotiate international agreements that impose limits on the practice.

There is, however, an underappreciated and counterintuitive sense in which replacing the old visa-based regime with a new data-based system can actually be *beneficial* for individual privacy—or at least certain aspects of individual privacy. In short, data-based screening eliminates the need for travelers to reveal the intimate details of their personal lives and finances through visa applications.

Visa applications normally require travelers to share a great deal of highly sensitive personal information with the government. For instance, applicants might be asked to indicate their marital status—including the potentially fraught matter of whether they are divorced—as well as the names and birthdates of their spouse and other family members. They might be asked to indicate their employer, school, occupation, and who will be paying for their trip, which can not only reveal their socioeconomic circumstances but also provide important insights into their social networks. The government might ask them for the address where they intend to stay during their travels, the names and contact information of the people they will be visiting, whether they have any relatives in the country, and the names and relationships of the people accompanying them—which, taken together, can paint a fairly clear picture of the social circles in which they move. Applicants might even be asked about their medical history, such as whether they’ve ever contracted a serious disease, suffered from a mental disorder, or been addicted to drugs.

In addition, visa applicants are often required to provide supporting financial documentation to demonstrate that they have the means to support themselves while traveling and are not likely to engage in illegal economic migration or require public assistance. They might be asked to turn over bank statements, which can reveal their general financial well-being as well as

the specific goods and services on which they spend their money, the charities and political organizations to which they contribute, and so on. Or the government might ask them to provide paystubs, again shedding light on their socioeconomic condition.

None of this highly sensitive information is required in a system that combines visa-free travel with data-based passenger screening. In its place, the emerging regime collects and analyzes comparatively innocuous pieces of information that travelers provide to airlines and other companies in the ordinary course of doing business—e.g., name, mailing address, email address, phone number, frequent flier number, seating preference (window or aisle), and similarly picayune data. PNR is hardly a dossier of passengers' most intimate secrets. It certainly seems far less revealing than asking a traveler to disclose, say, whether she is divorced or suffers from HIV. In this respect, then, the new data-centric regime can be seen as an unexpected advance for privacy values over its visa-based predecessor.

At the same time, however, it's not right to suggest that the emerging system is entirely without privacy costs. As Daniel Solove has observed, collecting and aggregating a large volume of seemingly innocuous pieces of information enables the government to generate new knowledge about people:

[W]hen combined together, bits and pieces of data begin to form a portrait of a person. The whole becomes greater than the parts. This occurs because combining information creates synergies. When analyzed, aggregated information can reveal new facts about a person that she did not expect would be known about her when the original, isolated data was collected.⁴⁰

In other words, compiling the individual tiles allows the government to piece together the larger mosaic.⁴¹ This is indeed the very point of large databases—aggregating information can yield new insights about travelers, both those that are helpful (such as inferences about travelers' possible ties to ISIS or other terrorist groups) and potentially harmful (such as inferences about travelers' private lives).

The move to data-based passenger screening thus represents a privacy tradeoff. The government asks travelers to turn over less personal information of obvious sensitivity, such as medical history and financial records. In its place, the government collects data that on its face is fairly innocuous, such as mailing addresses and frequent flyer numbers, which it then exploits to generate new and potentially revealing information about travelers. The sensitivity lies not so much in the information that is collected but in the new information that is produced. Privacy concerns thus migrate from the initial point of collection to subsequent stages where the data is analyzed and used; first-order privacy concerns are partially supplanted by second-order privacy concerns.

⁴⁰ Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 507 (2006).

⁴¹ Nathan Alexander Sales, *Mending Walls: Information Sharing After the USA PATRIOT Act*, 88 TEX. L. REV. 1795, 1806 (2010).

CONCLUSION

The two elements that combine to form the emerging regulatory scheme for international travel—visa-free movement of persons along with government analysis of personal data—are often seen as being in some tension with one another. There is an important sense in which this conventional wisdom is accurate. What seems like a permissive no-visa regime might not in fact be all that permissive if it requires big data to operate. But there is another, less obvious sense in which visa-free travel and data analysis do not work at cross purposes but actually complement one another—certainly when it comes to the economic benefits of mass international travel, but even in terms of individual privacy. For when this new regulatory approach is considered against the backdrop of the visa-based system it partially replaces, it become possible to appreciate its privacy implications more completely. Counterintuitively, by eliminating the need for travelers to complete visa applications that reveal the intimate details of their private lives, the new regime's reliance on airline reservation data can actually be beneficial for travelers' privacy.