7 Air Travel

The swift and affordable movement of people and goods is essential for society to function. Everyday people move around environments either through spaces that are increasingly monitored, augmented, and regulated by code or using modes of travel that are progressively more dependent on software to operate. Rather than discuss various different types of mobility, their infrastructure, and management, in this chapter we focus on how air travel has become dependent on software to take place (for a similar treatment of road transportation, see Dodge and Kitchin 2007a). Air travel consists of a passage through code/spaces that are governed by automated management. Tickets are bought online, whether individually or through an agent, check-in is automated and verified by unique passenger and ticket codes, security and surveillance rely on sophisticated captabases and sanctioned by pattern analysis programs, baggage transfer is sorted by bar code, planes are increasingly flown by computers and guided by air traffic control (ATC) systems, and immigration is verified by the scanning and processing of identification codes such as passport numbers and biometrics. The decision as to whether people and luggage can progress from one code/space to the next is more than ever before taken by systems that operate in an automated, autonomous, and automatic way (see figure 7.1).

These various coded infrastructures and processes entangle and fold together to form a vast coded assemblage that defines the practices and experiences of air travel. The relational problem to be solved is one of transferring people and goods from one location to another in a time-efficient, safe, and profitable fashion, and a key part of the solution is code. The whole apparatus of air travel, from initial transaction to exiting the airport at the final destination, is virtualized. As a result, the material transfer of people and goods has become *dependent* on the virtual. In this sense, air travel has become, in Castells's (1996) terms, a real virtuality *par excellence*, seamlessly blending the materiality and virtuality of travel.

That said, as we noted in chapter 4, how code/spaces are transduced in practice are contingent, relational, negotiated, and context dependent. Despite the desire of automated management to transduce an entirely observable, manageable, and predictable

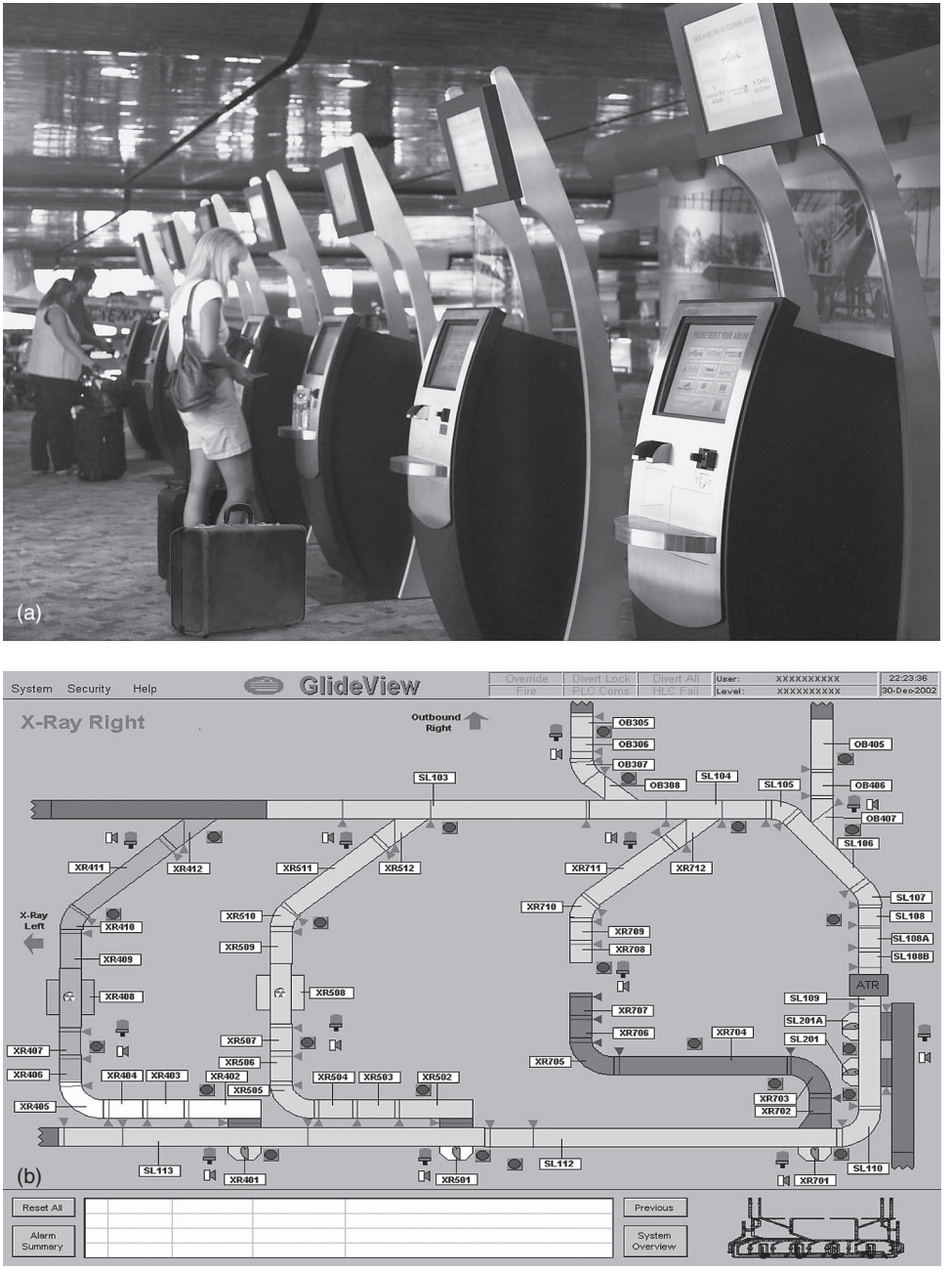


Figure 7.1

Visible surfaces of software in air travel. (*a*) Check-in kiosks with software interfaces. (*b*) Interface screen for a baggage handling system. (*c*) Cockpit view A320 airliner with multiple digital displays (*Source*: Guillaume Grandin, Air France). (*d*) View of the console of a U.S. immigration officer scanning a passenger's finger.

Figure 7.1
(continued)

assemblage, the code/spaces of air travel are not consistently produced, always manufactured and experienced in the same fashion. Rather, the connected sequence of airport spaces are beckoned into being in diverse ways, so that no one person's experience of moving through the sequence is identical to another, as it is shaped by the unfolding interactions between passengers, staff, material objects, and virtual systems. Consequently, air travel is never repeated exactly twice and never fully predictable or ordered. That is not to say that there is not a consistently repeating pattern and sense of order to the ongoing production of air travel, but it is to recognize that such patterns and orderly procession are mutable and open to rupture and resistance, and are reproduced through the citational performance of people, machines, and software systems designed to make air travel work in particular ways. As we illustrate below, even within the more software intensive transition zones, code/space is still negotiated—code is not simply law when people fly.

Transduction of Air Travel Code/Spaces

Air travel provides one of the key material supports to the global economic system connecting together people across a network that makes much of the planet accessible within twenty-four hours travel (for those who can afford it, and possess the right documentation and privileges). At any moment of the day, there are an estimated 1.5 million people in flight above the earth (Urry 2007). In many ways, the aviation industry has expanded in parallel to the growth in computing and information and communication technologies from the 1960s onward, drawing on these new technologies to improve efficiency, productivity, competitiveness, safety, and security. The result is that air travel is increasingly reliant on software engineering and networked computing, never more so than in the post-9/11 period, with its emphasis on creating a system that amasses voluminous amounts of capta about the people that pass through the assemblage in order to render it more safe and secure. Ironically, while code is used to make air travel more transparent to the authorities, how it is deployed is increasingly routinized and backgrounded, and many aspects remain invisible or unexplained to passengers and most employees. The progression of traveler from arrival at the airport to takeoff of the flight involves a whole host of processes and interactions between passenger (and baggage), the airline, and the state-sanctioned security apparatus (see figure 7.2). The result is that air travel consists of a passage through sequences of code/spaces.

In many ways, a passenger ticket is the material embodiment of code/space on which are printed several data codes, which while meaningful to the software programs that facilitate travel, are mostly meaningless to the passenger. With the move to e-tickets, these codes are often hidden further, reduced to a single unique code number that identifies the passenger at check-in. These capta's prime purpose is to

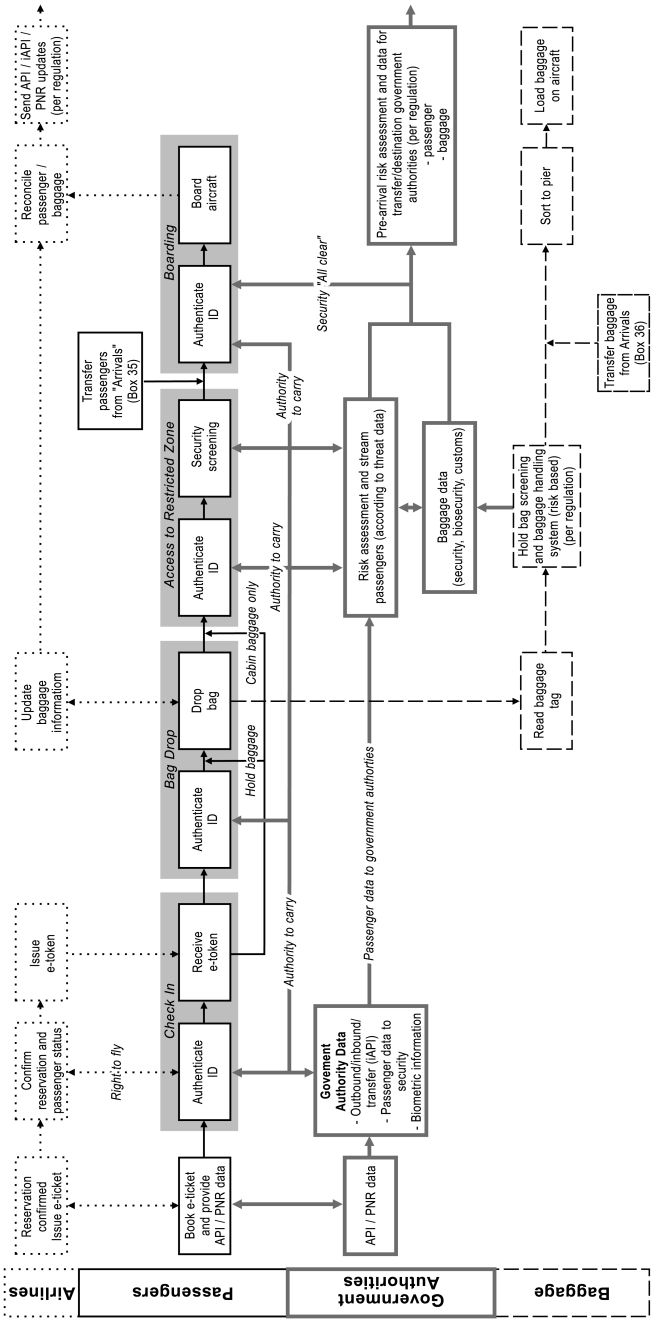


Figure 7.2
An inscription of orderly air travel created by an industry expert group called Simplifying Passenger Travel which shows the idealized flow in a typical passenger departure process. Many elements shown in this diagram are reliant on software. (Redrawn from SPT 2006, 5)

verify that the ticket holder and ticket match, and that the person is cleared to progress to the next stage as moving through the airport and onto the destination. Ticketing details are held as passenger name records (PNRs) (see figure 5.2), stored on a handful of global distribution systems (GDSs) (under such brand names as Sabre, Amadeus, Worldspan, and Galileo) which can be accessed from many thousands of terminals across the world. PNR content varies between booking systems, but usually includes a minimum of passenger name, reservation date, travel agency, travel itinerary, form of payment, and flight number. Many of the code numbers are unique identifiers and references to comprehensive customer management systems maintained by airlines, which profile passengers based on their frequent flyer status, and ticket class. Other forms of security profiling systems are increasingly being implemented to separate the risky (or potentially risky) from the safe (see below for particular examples in the United States; also see Bennett's 2004 detailed empirical attempt to trace some of the locations through which his personal capta flowed when booking plane tickets). It also important to realize that much of the algorithmic classification of passenger risk happens prior to arrival at the airport, with anticipatory governance seeking to forestall future threats before they materialize (Budd and Adey 2009). Of course passengers have little, if any, knowledge as to what risk and threat models have been applied to their pattern of travel, ticket purchasing, consumption, and lifestyle characteristics.

The reliance on ticketing codes in the PNR for check-in is the primary reason that a departure area is now a code/space. Simply put, passengers cannot be checked into a flight unless they can be successfully verified with respect to the check-in software system, either through an intermediary in the form of a human agent or through a self-service kiosk. If this system is down, then there is no other way of checking passengers and baggage in or allocating seats. Check-in agents are no longer trained or authorized to do manual check-in, and the destination airport would not accept passengers without a full manifest being electronically transmitted to them, nor would they accept baggage that cannot be uniquely linked to a particular passenger by way of a software generated ID code printed onto a bar code. The check-in area then is dependent on the check-in software. If the software fails then the space fails to be transduced into a code/space as it should be. Instead, the check-in area is transduced as a large waiting room that will soon become disordered and crowded as more and more passengers arrive, but cannot progress to the next space in the store-forward flow architecture of the airport (Fuller 2009; Kitchin and Dodge 2009).

Beyond check-in, passengers are forwarded through a security screening area to the "store" of the predeparture lounge (where they will hopefully consume products and services that are vital to profitability of airports). The screening area marks the beginning of a sterile zone that should be devoid of proscribed people, objects (knives,

scissors), and activities (filming and cell phoning). The security screening area is similarly a code/space, dependent on sensors to generate capta, and software to process and analyze it, along with human oversight to watch and interpret display screens, ask additional questions, frisk people deemed to be potential risks, and search bags. The boarding card bar code is often scanned for verification of identity; hand baggage is placed in a sophisticated x-ray machine that can visually slice through items; passengers are gazed upon by human eyes and also rendered "transparent" by channeling through metal detectors and new body scanners that use backscatter radar to look through clothing (Amoore and Hall 2009). Additional scans and tests can be done, such as using a GE EntryScan machine that blasts air onto a passenger's clothes and hair, capturing the particles driven off and automatically sniffing them for explosives and narcotics using an ion trap (GE Infrastructure Security 2007) or individually swabbing shoes and items within a bag for chemical residue indicative of explosives. Checked luggage takes a separate journey, usually through the bowels of the airport, and is also subject to software monitoring and automated scanning.

Once beyond the security area, the passenger is free to move around the store area of the predeparture lounge. This usually contains a mix of seating areas, shops, restrooms, and restaurants. In general, this area is produced as a coded space. Code makes a difference to the transduction of space, but is not essential to it (with the exception of certain retail processes which are dependent on software to handle payment transactions and manage their stock; see chapter 9). Here, passengers are subject to automated surveillance and airport management systems. They can also check the status of their flights via information screens, or use their cell phones or access Wi-Fi to communicate with the outside world. However, if these systems are down, the space still functions as a location to wait before a flight is called over the loudspeaker. Once the flight is announced, passengers walk to the relevant gate. Sometimes, they might pass through an exit passport control point to verify that they have permission to leave the country or enter the country they are about to fly to. At the gate, they walk onto the plane, again their ticket and identity are verified, and boarding cards are carefully scanned and tallied to confirm that the correct passenger numbers are on the aircraft.

Similarly, the plane itself is a code/space from the cockpit through to the in-flight entertainment system and digital maps displayed in the cabin. Over the past twenty-five years or so, avionics has dramatically changed flying for pilots. The increasing integration of sophisticated virtual geographic representations into the cockpit means that pilots now fly through real space virtually, using digital instruments (artificial horizons, inertial and GPS navigation), radio communications systems, real-time radar map displays, and so-called fly-by-wire controls, collision avoidance systems, and continuous feedback from onboard sensors and ground-based data streams. The Boeing

747-400, a leading long-haul jet aircraft, has some 400,000 lines of software code to power its numerous cockpit avionics systems, while the newer Boeing 777 aircraft has some seventy-nine different computer systems requiring in excess of four million lines of code (Pehrson 1996). The key control surfaces of the aircraft are not directly connected to the pilot's stick and peddles. Instead, commands are interpreted and approved by software before being physically enacted (see figure 7.3). Further, the pilot and plane's performance is continuously monitored and stored by black boxes, or flight data recorders. The flight itself takes place through the coded space of the atmosphere, which contains radio navigation beacons, GPS signals, and ATC systems that monitor all movements and direct planes on route to their destinations.

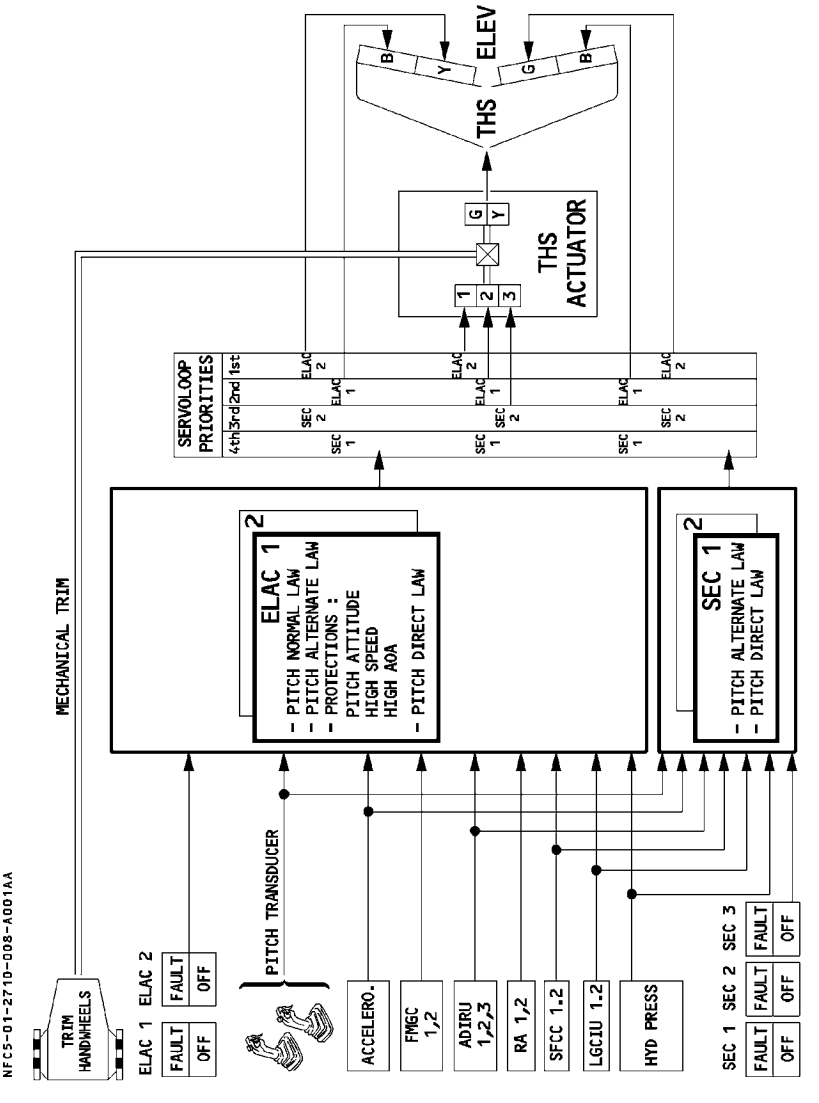
Once the plane has landed and the passengers have disembarked, they proceed to the immigration control hall. Here, their identity is verified again and a decision taken as to whether they can enter a country and under what conditions. We discuss the nature of how this verification occurs in more detail later in the chapter. Passengers then go on to baggage claim. In smaller airports, bags are taken from the plane to the carousel by hand. In larger airports, they are routed through mechanical systems that scan the bar codes on the bags and automatically direct them to the correct carousel. In the latter case, the baggage hall constitutes a code/space. If the code fails, the hall becomes a waiting area, not somewhere to collect bags and move on to the customs zone before exiting into the coded space of the arrivals hall.

Taken to their logical conclusion, we can think about the code/spaces of air travel extending to the Internet and the GDS systems through which tickets are purchased (travel web sites, booking databases, credit card encryption) and global financial markets (the networked spaces of banks, stock markets, financial districts, insurance centers) that, as the volatility across the aviation industry post-9/11 have demonstrated, play a large role in defining airline, airport, and aircraft manufacturers' viability and in restructuring routes, service levels, and plane production. The code/spaces described above are often simultaneously local and global, grounded through the passage of people and goods, but accessible from anywhere across the network. They are linked together across the whole architecture of networked infrastructure of air travel into chains that stretch across space and time to connect start and end nodes into complex webs of interactions and transactions that can be accessed from many thousands of terminals across the world. The massive assemblage of air travel is then widely distributed and diversely scaled.

Figure 7.3 (opposite page)
An illustration from a training manual for an Airbus airliner showing that lines of control from the pilot to the physical flight surface pass through the ELAC (elevator aileron computer) and SEC (spoilers elevator computer) where they are subject to algorithmic laws before being enacted. *Source*: www.smartcockpit.com/data/pdfs/plane/airbus/A320/systems/A320-Flight_Controls.pdf

PITCH CONTROL – SCHEMATIC

FOR INFO



Why Code/Spaces Are Always Incomplete

It is important to note that code/spaces of air travel have accreted over time to no set master plan, with technological advances, a changed political and legislative and economic landscape, to create an interlocking assemblage. The components of this assemblage have a diverse range of owners, maintainers, and licensing, accompanied by a labyrinth of contracts, leasing, and service-level agreements. Further, a raft of national and international bodies and industry organizations are responsible for the setting and vetting of standards for systems where software is vital (such as aircraft navigation and ATC systems). As a result, the assemblage emerges as a constellation of many, sometimes competing, interests.

Such an accreted assemblage is riven with nooks, crannies, and gaps in the system which make them necessarily incomplete in nature. This incompleteness is also revealed when the intended transduction of space fails, either through minor glitches or rarer, catastrophic incidents. Examples of the former are when luggage is lost or passengers are bumped off of a flight because of overbooking. Interestingly, in these cases it is common for airline staff to be at a loss to explain the cause, simply blaming the computer for the problem. Bumping is, however, not a system error, but the logical outcome of commercial pressures, wherein complex (proprietary) yield management algorithms work to maximize profits by ensuring planes fly as full as possible. These systems rely on notional behavioral rules and statistical models of passengers which assume that not all reserved passengers will actual turn up and want to fly. The very survival of an airline can depend on how well its yield management is working, as every empty seat is revenue lost. In terms of catastrophic accidents, the cause of many incidents which have been traced to so-called human error are more often due to the complexity of technical systems and a breakdown in human–computer interactions, particularly for pilots (Baberg 2001). Airline delays and flight cancellations also highlight the fragility of the air travel assemblage. Once ordered schedules begin to unravel, perhaps due to ATC problems or bad weather, then the smooth operation of the airport can quickly be disturbed. As the store-forward flows of passengers become interrupted, the airport environment quickly changes character, with crowds of annoyed passengers and, at the worst times, stranded people forced to sleep in departure lounges.

Despite these potential disruptions to the air travel assemblage, the danger is to think about the store and forward movement through its code/spaces in a deterministic (that code determines how the space unfolds) and universal manner (the same processes occur in all airports in the same way). This is clearly not the case. Airports emerge in diverse ways. Code is not law by itself (Lessig 1999). Software's ability to do work in the world is mediated by people—either through a direct interface between passenger and employee, or through gatekeepers who take the outputs of a program, interpret the results, and are able to negotiate with passengers or co-workers to varying

degrees. What this means, is that how travelers engage with software and its gatekeepers (the travel agent, check-in supervisor, security guard, and immigration staff), and react through embodied practice, varies between people and is contingent on their abilities, experiences, prejudices, and the context in which interactions occur. It is necessarily a social and cultural practice, not a simple, deterministic exchange or an act of raw governmentality, and it proceeds in multifarious, subtly mutating ways.

In this sense, the code/spaces of aviation are of-the-moment and performative. The ordering of flows in the store-forward nature of the airport assemblage in particular take continual tuning, and as Knox et al. (2005, 11) note from their study of a British airport, "the organization of 'flow' is always in danger of 'overflow,' of disintegration into confusion and flux, where people and objects become unstuck from the smooth operation of representations and get lost in the intransigent opacity of the 'mass'." Negating the occurrence of overflows, means the airport is remade continuously—cleaners clean; security guards patrol; food is prepared, served, cleared away; planes land, taxi, disgorge passengers and luggage, are checked, refueled, serviced, and reboarded, and they depart; travelers and their bags move through the various architectural spaces and inspection points, and are channeled in various ways (by signs and flight information display screens, by printed boarding cards, by audible announcements, by customer service agents, by automated barriers and doors). Airports require continuous routine maintenance, ad hoc repairs and planned renewal that is easily overlooked by passengers unless they are directly impacted (Graham and Thrift 2007). They exhibit metastability at different scales—"they are stable [only] in their constant instability" (Fuller and Harley 2004, 153).

Given this collective and incomplete nature, there is always scope for workarounds, as airport staff in different roles adapt their interactions with software systems to cope with the pressures of on-the-ground situations. Oftentimes these are unauthorized actions, undertaken with the tacit understanding of managers as necessary to circumvent systems in order to get the job done (for one example, staff may violate rules by sharing access accounts). There is also the ever present potential for errors, particularly in capta entry and translation within and between these software systems (see the numerous real-world stories reported on the RISKS List, http://catless.ncl.ac.uk/risks), while the output of software can easily be wrongly interpreted by workers and passengers (so-called human error). There are also opportunities for malicious damage to the vital software systems of air travel from insiders, and also external attacks. One example of this occurred in August 2006, when it was reported that a computer virus infected the US-VISIT immigration software system operated by the U.S. Customs and Border Protection Agency and caused considerable disruption to passenger flow (Poulsen 2006).

If one spends time in an airport observing what is happening, its diverse realities become all too clear (on the sociological interpretation of airports see Gottdiener 2001

and Pascoe 2001). Consider the example of checking in for a flight. The practices of checking in are not simply rote, but are part of a social exchange between the passenger, the check-in agent, and information systems. Passengers ask additional questions about their travel, for example, checking in to additional legs, or confirming the routing of baggage to the final destination. Check-in agents can ask for additional information, such as whether the bag was packed by the passenger. There can be frank exchanges between them when, for example, the system does not recognize the ticket or the passenger, or has seemingly lost details of pre-ordered seats. There is likely to be further exchange if the desk is closing as a late traveler arrives, or if the luggage is too heavy and the airline wants additional payment to carry it. Other examples of social exchange occur when the flight is overbooked and the airline is seeking to hold over or reroute passengers, or when the check-in agent will not check the passenger all the way through to a final destination, claiming a system glitch. These situations are resolved through a combination of dialog between people and accessing, updating, and modifying records of captabases.

Similarly, security checkpoints and immigration are *negotiated* zones of transition. Code is used to screen and identify passengers in the security area, but often with a human operator who is usually part of a team. The level of attention one receives is often gendered, aged, and raced (women, children, and Caucasians are generally perceived as less of a potential risk in the West), and agents have the authority to decide which items are confiscated and who receives extra screening (Parks 2007). These kinds of collaboration and negotiation are captured by the description below, drawn from observant participation research (Kitchin and Dodge 2009, 104–105).

> The bag belonging to the passenger behind is moved into operator's frame. The operator performs a set of scans. He zooms in on one section, then zooms back out again, and performs the same scan routine. He then zooms back in once more and calls a colleague over. Pointing at the screen he indicates the suspected problem and they confer. The colleague then gestures to the bag's owner, a smartly dressed man in his fifties and they head off to one side. The bag is placed on a counter and the passenger is asked some security questions and for permission to search the bag. The man concurs and all the bag's items are emptied onto a counter. The offending item is a meter-long steel security cable. There is a brief negotiation, where the security official clearly sees the cable as a potential weapon and the passenger argues that it is simply for securing the laptop to a workstation. The official concedes that the man can keep the cable this time, but suggests that it not be carried in carry-on luggage in future. One is very much left with the impression that not every passenger would have been allowed to keep the cable (and there is a large perspex box nearby full of confiscated items, including cutlery, penknives, nail files, a metal ruler, a hammer, and other assorted, mostly metal, objects).

While the processes and practices are broadly similar for all passengers, they emerge in contingent and relational ways, and by no means is the code simply law. As a result, as Wood (2003, 337) notes, the security screening area can be viewed as a form of

theater, consisting of the "spectacle of the frisk," within which, "we find ourselves tied within a web of individuation and de-individuation marked by perpetual surveillance." Likewise, when individuals pass through an immigration hall, they are subject to verification and examination. Here, machine-readable passports and, depending on location, biometric information are scanned, processed, and interpreted, with the results screened to gatekeepers (immigration officials), but not shown to the individuals themselves. The gatekeeper then decides whether a person gains entry to the country, often asking clarifying questions about the purpose of the visit, length of stay, and itinerary. Code is critical to the process, and is not easily overridden, but the decision is ultimately made by a person interfacing with software, sometimes in negotiation with the passenger. In the next section, we examine how new systems and procedures seek to minimize human interjection, and subject security and immigration to the law of code through the deepening role of automated management.

Automated Management of the Air Travel Assemblage

The use of software to manage passenger flow through the assemblage of air travel, along with a panoply of other routine but foundational management tasks, like aircraft scheduling, staffing levels, and accounts and payments, has a relatively long lineage. Such systems were originally used to make the business of air travel more efficient, competitive, and profitable. More recently, they have been used as a means to manage and regulate passengers and workers, especially in relation to security. Software enables airports, airlines, and states to identify, survey, and assess passengers and workers for potential risk, and to script air travel into more knowable and ordered environments. The aim is to render passengers and staff, in Foucault's (1978) terms, "docile bodies"; bodies that occupy the assemblage in an orderly, noncomplaining, compliant manner through visible systems of discipline (unique identification check-in and immigration, surveillance cameras, security checkpoints, warning signs, and architectural design), accompanied by a sliding scale of sanctions (delayed flight, termination of a journey, police questioning, arrest, criminal charges, threat of fines, and imprisonment). Both capture and automated surveillance systems are in evidence, often in conjunction with each other (see chapter 5).

Both passengers and employees are subject to capture systems. For example, as noted above, check-in can only be accomplished through the use of the check-in software system and the updating of PNR in a captabase. While check-in is a negotiated practice, the nature of the task is defined to a high degree by the software system that scripts the process. For the airline employee at a check-in desk, their activity is reshaped to that demanded by the sequence of prompts and commands generated by the system. Unless all of the required information fields are entered, the passenger cannot be successfully checked in to the flight. Moreover, the system captures much

more than the passenger's details, but is also the means by which workers can be surveyed with regard to quality and quantity of their work. Similarly, the passenger using a self-service kiosk is directed through a sequence of screens and questions that must be answered appropriately. Their activity is entirely scripted and over-determined by the system, with appropriate capta collected (although see Kitchin and Dodge 2009 for examples of resistance). These capta are processed and evaluated using sophisticated algorithms that compare the records with various customer and security captabases, combine it with other known capta about a person, assess the passenger's status, and react appropriately (issue or deny a ticket, provide upgrades and access to airline lounges, or target for special security checks and questioning). These systems are automated, automatic, and autonomous in nature. For example, an iris scanner generates and evaluates capta, and has the authority to authorize passage without human oversight.

The development of such automated management systems, especially those related to security and immigration, has expanded dramatically post 9/11, alongside moral panics concerning illegal immigration and asylum seekers. Here, the aim is to upgrade the effectiveness of systems by introducing new grammars of action that deepen capta input and improve analysis, identify and deny potential security risks before a crime is committed, anticipate threats and predict future passenger behavior (Adey 2009; Graham and Wood 2003). In the United States, these systems include the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT), APIS (Advanced Passenger Information System), and Secure Flight programs. Elsewhere, equivalent systems are being developed; for example, in the UK there is the "e-Borders program" and in Canada, "Smart Borders." These systems use software with the aim to strengthen border controls by more reliably identifying and classifying people prior to and as they travel, verifying their departure, and building up a profile of individual movements over time. Here we outline in brief the three U.S. systems (as they operated or were planned in 2005; note these systems are subject to rapid change).

The US-VISIT system is operated by the U.S. Department of Homeland Security (DHS) and aims to automate the regulation of the flow of non-U.S. citizens in and out of the United States. For those needing a visa to travel to the United States, biometric data (digital fingerprint scans and photographs) is a key form of capta, collected at the point of application (usually a U.S. Consulate office in the country of origin) and checked against a system of interlinked captabases for known criminals and suspected terrorists. When the traveler arrives in the United States, the same biometrics are used to verify that the person is the same one that received the visa. For countries who have a visa waiver program (most OECD nations), travelers must travel with a biometric passport or be photographed and fingerprinted on entry. At its core, the system consists of the integration of three existing DHS systems: the Arrival and Departure Information System (ADIS), the Passenger Processing Component of the Treasury

Enforcement Communications System (TECS), and the Automated Biometric Identification System (IDENT) (DHS 2004). US-VISIT has a one-hundred-year capta retention period and the capta are shared with "other law enforcement agencies at the federal, state, local, foreign, or tribal level" who "need access to the information in order to carry out their law enforcement duties" (DHS 2003, cited in Privacy International 2004). Indeed, the capta US-VISIT generates is used for:

> Identifying, investigating, apprehending, and/or removing aliens unlawfully entering or present in the United States; preventing the entry of inadmissible aliens into the United States; facilitating the legal entry of individuals into the United States; recording the departure of individuals leaving the United States; maintaining immigration control; preventing aliens from obtaining benefits to which they are not entitled; analyzing information gathered for the purpose of this and other DHS programs; or identifying, investigating, apprehending and prosecuting, or imposing sanctions, fines or civil penalties against individuals or entities who are in violation of the Immigration and Nationality Act, or other governing orders, treaties or regulations and assisting other Federal agencies to protect national security and carry out other Federal missions. (Federal Register 2003, cited in Privacy International 2004)

The final statement, "and carry out other Federal missions," effectively means the capta can be used for whatever the U.S. government thinks is appropriate now and in the future; this clearly opens the door to wider surveillance of mobility. Further, this sharing of capta across agencies makes it available for use by several hundred mining programs identified by the General Accounting Office in U.S. government departments for purposes beyond security and immigration, and clearly raises issues concerning function creep, privacy, and civil liberties (Privacy International 2004).

In addition to US-VISIT, passengers on international flights to the United States are prescreened by U.S. Customs and Border Protection using APIS. APIS uses information from the machine-readable part of a passport, along with PNR information supplied by air carriers (this links to other layers, such as, international standards in the capta ontology of passports determined by the International Civil Aviation Organization.) APIS requires passengers to provide in advance to U.S. Customs details such as name, date of birth, sex, travel document number, and destination. APIS targets suspected or high-risk passengers by checking for matches against a multiagency database, the Interagency Border Inspection System (IBIS), and the FBI's National Crime Information Center wanted persons files. IBIS includes the combined databases of U.S. Customs, U.S. Immigration and Naturalization Service, the State Department, and, most likely, multiple other federal agencies.

The Secure Flight program monitors internal flights, and accordingly U.S. citizens. Secure Flight is the replacement for the CAPPS (Computer Assisted Passenger Prescreening System) program, with the main differences being that the system only looks for known or suspected terrorists, not other law enforcement violators, that it includes a redress mechanism if passengers believe they have been unfairly or incorrectly selected

for additional screening (Sternstein 2004), and it does not have new capta requirements for airline reservations systems. Using PNR capta, Secure Flight verifies the identity of the passenger and conducts a risk assessment using commercial and government data, and updates the Transport Security Agency's (TSA), Passenger and Aviation Security Screening Records (PASSR) captabase (Hasbrouck n.d.). The risk assessment affects the passenger's assigned screening level—no risk, unknown or elevated risk, or high risk. Based on the risk level, the traveler could be subjected to additional searches, questioned by screening staff, or detained and interrogated by police. Importantly, the rules of grammar that lie at the root of these determinations are purposefully secret, being classified as "Sensitive Security Information" and, as such, are not open to scrutiny (in terms of independent verification of their effectiveness) or informed challenge (in terms of equity issues, such as potential racial profiling).

It is fair to say that these automated management systems have been subject to some expressions of concern and criticism. For example, CAPPS was criticized on normative grounds and replaced due to the ease with which the "system could be beat with fake identification, the system's reliance on commercial databases widely acknowledged to be riddled with errors, and the fact that the system compromised the privacy of airline travelers without making nation's airliners safer" (DHS 2004). In 2004, the American Civil Liberties Union published a list of seven reasons to question the design and deployment of such automated passenger screening and profiling systems (ACLU 2004). These reasons focused on errors, due process, cost, and impact.

First, passengers are judged in secret and without knowing the terms by which they are judged. Second, as the TSA itself acknowledges, these systems are not as infallible as their developers suggest, being open to both biographical and biometric errors. For example, biographical errors include recording mistakes, such as misspelled names and incorrectly keyed dates of birth, nonupdates (change of address), missing or misleading fields, and mismatching errors and false positives, especially based on names. These errors are particularly prevalent in commercial databases sometimes used as a component in profiling systems. Biometric errors include the "failure to enroll rate," wherein the biometric is either unrecognizable or not of a sufficiently high standard (worn fingerprints), a "false nonmatch rate," wherein a subsequent reading does not properly match the enrolled biometric (facial aging), and false positives, wherein a system is so large that there are many near matches leading to people being falsely identified. In 2005, the TSA was predicting an error rate of at least 4 percent, seriously undermining the effectiveness and integrity of the system (for every hundred million who fly, four million people will have errors in their capta that could adversely affect their ability to travel) (Kitchin and Dodge 2006).

Third, with respect to due process, the ACLU (2004) points out that findings are largely nondisclosed and there is a limited process of notification, correction, and appeal. Fourth, these new systems place an unnecessary burden on commercial air-

lines, travel agents, and the public by passing the costs of a flawed and ineffective security system onto them. Fifth, the systems infringe on privacy through the creation of lifetime travel dossiers that remain beyond the control of the individuals that they relate to. Sixth, they have the potential to foster the systematic unequal treatment of passengers on the basis of some arbitrary criteria (the so-called flying while Arab effect, where those of Arab or South Asian descent are subject to extra screening and profile based simply on race and ethnicity indicators in their capta shadows). Seventh, there is great potential for control creep, that is, capta being used for purposes beyond its original collection, and the system being rolled out to govern access to other kinds of environments such rail networks, national monuments, and key public buildings (Graham and Wood 2003; Lyon 2003).

Taken together, US-VISIT, APIS, and Secure Flight aim to create a capta shadow of travel for individuals that lasts a lifetime. In short, all air (indeed international) travel will be collected and linked to biographic and biometric information and used to screen individual travel behavior. These systems are representative of the capture model, wherein the grammars of action are the formalized rules of assessment at the heart of the classification and risk assignment process, and biographic and biometric capta are the basic ontology. Clearly, these systems actively shape, both implicitly and explicitly, the nature and procedures of travel (rather than simply externally surveying moving bodies). In explicit terms, travelers have to acquire machine-readable passports, repeatedly submit to biometric capta generation, and potentially experience extra security and immigration checks. In implicit terms (to travelers at least; explicit to workers), how the travel industry is organized, its procedures, operations, and work practices, are altered in ways not necessarily democratic or equitable to those directed affected.

As noted above, while these systems of automated management seek to create an exhaustive and infallible means of regulating air travel, they are open to negotiation and resistance. The drive is to limit such negotiation through improvements in system design and capta quality, that provides both passengers and workers fewer opportunities for finessing or overriding the work that code does, and which further empowers code to determine outcomes. Resistance is being tackled in a different way, through the creation of a powerful discursive regime that brings both passengers and workers in line with its logic.

The Discursive Regime of Travel Code/Spaces

The code/spaces of air travel, and the regulatory capacity of automated management, are supported by at least seven interlocking discourses. These are security, safety, antifraud, citizenship, economic rationality, convenience, and free skies. These discourses work ideologically to construct and position code/space as a commonsense method:

it benefits passengers and workers, society and the aviation industry alike, with few negative externalities (and these are more than outweighed by benefits).

Major airports and passenger aircraft have been, and continue to be, perceived as prime targets of terrorism. They are a means of international travel and smuggling for terrorists and criminals. Further, planes are involved in accidents, hijackings and attacks. Code/space, it is argued, is desirable because it creates a more secure and safe environment. Automated management allows the surveillance of passengers and workers to become more panoptic in scope, both widening and deepening the extent to which the complex and dynamic flows of air travel can be policed, thus making air travel a more secure and safe undertaking. Part of the power of code/space is what Foucault (1988) calls a "technology of the self": a sociospatial configuration where the presence of a technology persuades people to self-discipline their behavior; to act in ways prescribed by those controlling the space and technology. In the case of airports, this is reinforced through regular auditory security warnings about unattended baggage, check-in security questions, warnings not to tamper with the restroom smoke detectors, barriers, and access controlled doors, and blanket CCTV coverage.

Safety is not tied to security alone. There are other ways that automated management ensures safe passage. For example, the use of software is now integral to effective air traffic control—code reduces the physical and cognitive demands on pilots, and provides a means of remote detection and automatic response to system failures. Further, airlines stress their maintenance record, and the aircraft manufacturer's competence, based in part on the allure of digital systems.

Safety and security have often been accompanied by discourses of anti-fraud and citizenship, and indeed in some cases they have been explicitly linked. Here, the systems are seen as a means to enhance the effectiveness of policing state borders and to ensnare and return illegal immigrants and asylum seekers. For example, a press release for the Project Semaphore (the precursor to the e-borders program), UK Immigration Minister Des Browne stated:

> e-Borders, along with biometric ID cards, shows how we are using new technology to develop embarkation controls for the 21st century. Access to information about passengers before they travel will help in the fight against illegal immigration, particularly document and identity abuse. It will also aid law enforcement and counter terrorism. At the same time, technology will allow us to speed through low risk passengers, helping British business and visitors to the UK. (UK Home Office 2004)

These interlocking discourses of anti-fraud, citizenship, and security are powerful because they are designed to enhance trust and confidence in the air travel industry as a whole, and address the concerns of legitimate, law-abiding citizens about illegal immigrants and bogus asylum seekers. Here, automated management is positioned as the foundation for confidence by providing infallible systems. Here, virtual code offers a solid solution to problem of porous, real borders. These discourses are further rein-

forced by government regulations, legislation, and a raft of international treaties (Butler 2001; Graham 1995; Van Zandt 1944).

Another set of discourses justifies the intense deployment of software by contending that it produces a more convenient or cost-effective journey. The transduction of code/space reduces the hassles of flying, and passengers supposedly gain through lower fares and faster progress through the airport. People can book online by themselves, meaning they do not have to interact with an agent, they can pass more smoothly and time-efficiently through the airport, and the systems can automatically acknowledge status such as frequent flyer, offer seating selection, and provide upgrades. The rhetoric produced contends that by automating aspects of the industry, airports and airlines can reduce their fares and fees, passing on savings to customers, while at the same time improving their profitability (a win-win situation). Further, code/space is economically rational because it facilitates global trade and tourism, creating and maintaining wealth creation for many. Here, code/space seduces people to its logic. In Althusser's (1971) term, code/space thus interpellates people to its ideas by enticing them to subscribe to and desire its logic and to willingly and voluntarily participate in its ideology and practice (rather than simply disciplining them into docile bodies).

This interpellation is key to another discourse, that of free skies, which paradoxically undermines the discourse of security. The ethos of air travel, from its very beginnings, has been one of freedom of the air and open skies. Implicit in the rhetorical messages of aviation is the deeply utopian logic that making the world a smaller place, will make the world a better place. Air travel is presented as a benevolent force that is inherently good for commerce and can bring greater understanding between people. The aviation industry strives to portray an image that it transcends geopolitics of the terrestrial world and offers travelers who can afford it an uncomplicated world without frontiers. The commercial aircraft manufacturers and major airlines spend heavily on marketing and advertising to promulgate this powerful, idealistic rhetoric, often utilizing universalist, visual tropes of the globe and world route maps (Cosgrove 1994). Code/space is now promoted as an integral part of making such utopian rhetoric a (profitable) reality.

While undoubtedly the aviation industry and its attendant code/spaces have detractors, it is fair to say that, at present, intensive software solutions are the hegemonic production of space associated with air travel. Indeed, given the potential for capture errors, flaws in procedures and structures, and potential impacts and misuses of the system, there has, to date, been remarkably little mass, organized resistance by individuals, unions, or activists to embedding of code into air travel. The resistance that has occurred is either expressed in disquiet, individual resistance, such as boycotts of travel to particular destinations, or legal challenges to state policy by groups such as the American Civil Liberties Union. This resistance, however, is a long way short of a

tipping point, wherein opposition becomes so great that it starts to challenge the present hegemony and places pressure on governments, airport operators, and airline managements to modify or abandon software systems. We posit that this lack of overt, organized resistance is due to five reasons detailed in chapter 5 (people have been persuaded to the new emerging logic; the changes occurring are viewed as simply an extension of an existing systems; new grammars of action and surveillance are seen as an inherent part of the system; the point of contact for most travelers is relatively painless; they are worried about the consequences of protest).

Conclusion

Aviation consists of chains of code/spaces. Software purposefully mediates many of the processes and actions of passenger movement. However, code is not simply law—deterministic, fixed, and universal. Rather, air travel emerges through the interplay between people and software in diverse, complex, relational, embodied, and context-specific ways. Even when flying becomes routine for commuters, it is an event that unfolds in multifarious, ever-changing ways. Because airports are diversely (re)produced, through the collaborative manufacture of people and code, they are certainly not the nonplaces as described by Augé (1995). While airports share similar architecture and processes, they are places in the same sense that small towns are, albeit with a daily flux of a large transient population. They have diverse social relations and formations, engender meaning and attachment, and represent different values and images of the locale and nation (Crang 2002). This is especially the case for the hundreds or thousands of workers, and for travelers who live locally and pass through the airport regularly; for example, Santa Barbara, California's airport with its small number of regional flights per day is very different from Chicago O'Hare with its thousands.

The widespread use of software to organize, manage, and produce air travel is set to grow further, supported by a persuasive set of discourses that work to create a powerful logic. These discourses include security, safety, economic rationality, and increased productivity, and convenience and flexibility. Software enables securer and safer air travel by widening, extending, and automating the degree to which passengers, workers, equipment, planes, and spaces are monitored and regulated through "infallible" systems of detection and response; software enables the streamlining and automation of myriad routine tasks, speeding up processes, increasing throughput, improving efficiencies, and reducing staffing and resource overhead that can be passed on to the traveler (or to shareholders); and software can provide passengers with greater convenience and flexibility in terms of booking, itineraries of travel, progress through the airport, requesting certain seating, and racking up rewards. Collectively, these discourses work to justify further investment, to make code/spaces appear as

commonsense responses to particular issues, and convince travelers (and workers) of the logic of their deployment. In other words, they work to ensure that air travel will consist of ever more densely interconnected code/spaces.

Despite these efforts to further deepen deterministic forms of automated management, the code/spaces of air travel will continue to be contingent and relational in nature, the products of complex and diverse interactions between people and code. As such, we believe these interactions warrant further attention and study, requiring detailed ethnographies of aviation across peoples (passengers by class, race, gender, age, disablement, and different kinds of workers), types of airports (local, national, and international hubs) and in a range of nations (with differing political economies, state policies, legislation, and business practices).