First Monday, Special Issue #7: Command Lines: The Emergence of Governance in Global Cyberspace

PEER-REVIEWED JOURNAL ON THE INTERNET

Software and the mundane management of air travel

by Rob Kitchin
and Martin Dodge

Over the past thirty years, the practices of everyday life have become increasingly infused with and mediated by software and captured in code. Software is increasingly embedded into objects and systems as a means to enhance and manage usage and to link together disparate and distanciated parts of an infrastructure, enabling new and refined processes. In some cases, such as air transportation, this embedding has become so pervasive and vital that if the software crashes one part of the system grinds to a halt, subsequently disrupting other aspects of air travel. In this article, we examine one part of this system, the profiling and screening of passengers, to argue that the use of software has engendered a new form of governmentality — mundane management — that is having a profound effect on the operation and regulation of air travel. The development of distributed information systems has enabled governments and air travel businesses to capture, cross–reference and regulate the ongoing status of individuals in ways that were previously difficult, if not impossible. By linking these capta together, a dense rhizomic assemblage of power/knowledge is being created; what is at best oligoptic (partial and selective) in nature is becoming more panoptic (all–seeing). This is especially the case given the trend towards increased granularity (resolution) and uniqueness (unique identification based on biometrics) of capta, and the fact that capta stored are unlikely ever to be deleted. These systems are not without their problems, particularly with regard to civil liberties. However, new procedures and technologies have largely been greeted by the public with ambivalence or welcomed, rather than resisted.

Contents

The power of code

Over the past thirty years, the practices of everyday life have become increasingly infused with and mediated by software and captured in code. Whatever the task or the realm — domestic living and the home, working and the workplace, consuming and sites of leisure and consumption, traveling and modes of transportation, communicating and technologies of communication — software makes a difference to how everyday life takes place. Software is increasingly embedded into objects and systems as a means to enhance and manage usage and to link together disparate and distanced parts of an infrastructure — to make life easier, more productive, more competitive, more value–added, and so on. It also enables new and refined processes, for example through the generation, storage, profiling, screening and communication of capta [1] about individual passengers (Dodge and Kitchin, 2005). In some cases, such as air transportation, this embedding has become so pervasive and vital that if the software 'crashes' one part of the system grinds to a halt, subsequently disrupting other aspects of air travel. For example, software is essential to booking flights, checking–in, security checks, planes' systems, air traffic control, processing immigration and customs, which when taken together form a coded assemblage that defines the practices and experiences of air travel (Dodge and Kitchin, 2004).

In this paper, we examine one part of this system — the profiling and screening of passengers — to argue that the use of software has engendered a new form of governmentality (how populations are managed; consisting on the one hand the techniques and practices of government, and on the other the discourses that rationalize and legitimate them) — that we term mundane management — that is having a profound effect on the operation and regulation of air travel. In short, software changes how passengers are managed and regulated because the development of distributed information systems have enabled governments and air travel businesses to capture, cross-reference and regulate the ongoing status (across dimensions of their choosing) of individuals in ways that were previously difficult, if not impossible, especially for whole populations. Information systems and the software for analyzing them provide a means of representing, collating, sorting, categorizing, matching, profiling, and regulating individuals; of generating information, knowledge and control through processes of abstraction, computation, modeling and classification (Dodge and Kitchin, 2005). By linking these capta together a dense rhizomic assemblage of power/knowledge is being created; what is at best oligoptic (partial and selective) in nature is becoming more panoptic ('all—seeing'). This is especially the case given the trend towards increased granularity (resolution) and uniqueness (unique identification based on biometrics) of capta, and that capta stored is unlikely to ever be deleted given the ease and the falling cost of capta storage (Dodge and Kitchin, 2005). These systems are, we contend, not without their problems, with particular potential dangers with regards to civil liberties (*e.g.*, privacy and discrimination). And yet, new procedures and technologies have largely been greeted by the public with ambivalence or welcomed, rather than resisted.

In order to make sense of this new mode of governmentality in the next section we examine two theories concerning the generation and use of information about individuals the surveillance model and the capture model, formulating a new hybrid capture–surveillance model. We then illustrate this model with respect to new passenger screening and profiling programs. In the final section we highlight some of the concerns about the development of such programs and hypothesize how they have quickly become hegemonic in status, ambivalently accepted and little resisted by passengers, before drawing some conclusions.

Mundane management

Governmentality has clearly been a consistent feature of societies for millennia. Further, it is clear that the rationalities, processes and mechanisms of governmentality change periodically given the invention of new technologies, new modes of economic production, or the development and growth of new ideologies. In some cases, the shift from one regime to the next is gradual and seemingly benign with limited overt resistance (*e.g.* the Enlightenment transfer from a feudal system to more modern state bureaucracies; Higgs, 2001). In other cases, the attempted shift to another form of governmentality is more violent resisted or bloody in its execution and maintenance. Here, we are interested in the former, the seemingly banal or ambivalent introduction and acceptance of a new mode of governmentality and its quick positioning as a hegemonic formation; that is, how new forms of capta generation, its analysis and application, along with new moral, political and cultural values, become accepted as the 'natural' and dominant order; how new practices ideas, beliefs, and values of governmentality come to be seen as desirable, inevitable, taken–for–granted and commonsense, even if they have (potential) negative consequences for many.

Foucault's genealogies (1976, 1978) sought to trace the development of a new mode of governmentality in the nineteenth century, charting the shift from feudal to modern society. Foucault details the development of new apparatus of governance, underpinned by sophisticated, objective, universal and 'scientific' technologies (including national censuses and the routine collection of health records, school attendance, criminal records, tax records, registration of births, deaths, marriages, and so on). These apparatus, Foucault argues, sought to create a statist, panoptic gaze cast upon a nation's citizens, working to manage and discipline them mainly through a self–disciplining effect. This effect is best illustrated through Foucault's discussion of Jeremy Bentham's panoptic prison. In this prison design, prisoners occupy cells that are always visible to a prison guard. However, prisoners do not know if the guard is watching or not, but are conditioned into self–disciplining their behavior given the threat that they might be under surveillance.

These systems are, we contend, not without their problems, with particular potential dangers with regards to civil liberties (*e.g.*, privacy and

discrimination). And yet, new procedures and technologies have largely been greeted by the public with ambivalence or welcomed, rather than resisted.

Foucault posits that the practices and technologies of this new mode of surveying governmentality became hegemonic because they were mobilized, supported and made rationale through a powerful set of discourses, which disciplined individuals to its logic. These discourses fused knowledge with power to create a powerful discursive regime. In Foucault's account, a discursive regime succeeds in maintaining the hegemonic status quo because it creates a disciplinary grid that makes it difficult to challenge. That is, the discourses that maintain the hegemony effectively neutralize acts of resistance by ensuring that resistive acts are judged on the terms of the hegemony (in this sense, freedom fighting is always judged as terrorism; nomadic is always judged in opposition to sedentary), and new forms of governmentality induce modes of self–disciplining as well as disciplining. In other words, the hegemony becomes the norm by which acts are judged, including by those who resist.

It should be noted however, that, *contra* Foucault, hegemonic surveillance formations are not simply reproduced through disciplining people to their logic. Indeed, we would argue that the much of the power of their discursive regimes stems from their seductive qualities (see Dodge and Kitchin, 2005). Following Althusser (1971), we would suggest that a discursive regime induces a process of interpellation wherein people willingly and voluntarily subscribe to and desire its logic. This is because a mode of governmentality is always productive — its makes society (feel) safer, more efficient, healthier, reduces transaction costs, and so on. Its disciplining effects are a price worth paying for most citizens due to its associated real benefits. These benefits are often positioned as forms of empowerment, for example how CCTV surveillance is positioned *vis–à–vis* women's safety.

The discussion, so far, has considered governmentality as underpinned by surveillance that seeks ultimately to create a panoptic gaze that discipline subjects. Following, and extending, Agre (1994), we think it profitable to broaden this view and to recognize new techniques of governmentality with regards to individuals, and information concerning them, that are better characterized through a model of capture. Agre (1994) posits that the surveillance model is a statist, centrally organized, and externally operated set of systems for gathering information about people. That is, the information collected is usually for the purposes of governance, a state organization is responsible for collating, sorting and managing the information, and the mode of surveillance is separate to what is being surveyed (*e.g.*, a camera system monitoring a workplace). The capture model recognizes a fundamental shift in how information is gathered, by whom, and for what purposes. The capture model acknowledges that the mechanisms by which information is gathered is increasingly an integral part of the same system that they seek to monitor and regulate (*e.g.*, a computer operation system logs its own use by an individual) and that these mechanisms in turn re–define and re–configure that system (e.g. change workplace practices), quite often in real–time. Agre (1994) argues that this modes of informational capture is possible because a grammar of action (formalized rules) has been imposed on a system. A grammar of action is a means of systematically representing aspects of the world, an organized language for modeling human behaviors. They lie at the heart of systems that utilize computing — databases consist of variables that represent people and things, and software is inherently rule–based, formalized and designed to process and model information. In other words, software code are grammars of action. Agre [2] notes that "once a grammar of action has been imposed upon an activity, the discrete units and individual episodes of the activity are more readily identified, verified, counted, measured, compared, represented, rearranged, contracted for, and evaluated."

If the grammar provides the rules by which the system works then the capta ontology supplies the accompanying vocabulary. The capta ontology refers to what information is collected (capta fields), its representational form, and how it is structured. In most computational systems capta are specified fields (*e.g.* age, gender, etc.), the representational form are digital identification codes, and they are structured into relational databases. The ontology defines the limits to the system as a system can only process what it captures and represents. As noted above, many facets of everyday life are now mediated by software and information systems, with aspects captured, given representation form, and processed by grammars of action.

Within the capture model, the disciplining of behavior is integral to the system as it is an inherent aspect of the grammar of action — it actively shapes how the system is used. For example, the use of an online airline booking system recasts how tickets are bought — the nature of the activity changes. This, in turn, "re–orders behavior so that it is more amenable to capture." [3] In other words, grammars of action necessarily structure activity. A recent example of this in the U.K. is the switch to "chip–and–pin" in authorizing payment card transactions where traditional surveillance verification of the signature by the cashier has been replaced by grammar of action determined algorithmically by pin number. That said, as Agre [4] notes, there is always some flexibility: "people engaged in captured activity can engage in an infinite variety of sequences of action, provided these sequences are composed of the unitary elements and means of combination prescribed by the grammar of action." Further, unlike the surveillance model where techniques of power are permanently visible, if discontinuous in action, to ensure the automatic functioning of power within the capture model they are often hidden and unknown, and thus more subtle in their effects [5].

The shift from a surveillance to capture model is technologically (the mode of capture is reliant on software code that can operationalise capta ontologies and the grammars of action) and market driven (wherein information is recognized as both a product and representation). Whereas information in the surveillance model is seen to be centralized and for the purpose of disciplining, within the capture model information is seen as diverse and for many purposes (including for commercial purposes, to create competitive advantage, increase efficiency and productivity, and so on, not simply regulation), often locally organized, and structured and used by single or select institutions. Agre (1994) draws five distinctions between the surveillance model (as typified by Foucaultian analyses) and the capture model, to which we have added several more (see Table 1).

Table 1: Contrasting the surveillance and capture models

Parameters	Surveillance model	Capture model
Metaphor	Vision	Linguistic
Site	Collection of information external to a system	Capture of information inherent to a system
Extent	Selective, but threatens exhaustive	Exhaustive
Mechanism	Disciplines through self–disciplining	Manages by reshaping activity
Visibility	Always visible	Often hidden, sometimes deliberately secret
Capta	Collected information is representation	Captured information is representation and product
Agency	People operated (*e.g.* somebody watches the camera or reads the file)	Software operated (*e.g.* automated)
Viewfield	Static (at fixed points with fixed views)	Typically distributed and increasingly mobile
Temporality	Partially dynamic, usually used retrospectively	Dynamic — updates and potentially regulates in real–time
Organization	Centrally organized and structured (statist)	Diverse, locally organized, institutionally structured (network)
Predictability	Non–predictive	Sometimes predictive, facilitates simulation

We would posit that while the surveillance model is legitimated through a discursive regime that is politically (statist and centrally) driven, that the capture model is championed predominantly through an organizational and economic regime that is more diffuse and localized (forwarded by groups and sectors with vested interests). Further, given that grammars of action are an inherent (constituent) part of a system they are less easily opposed than perhaps the imposition of a separate system might be. Together, the strong, overlapping legitimating regimes, and the sense that monitoring and regulation is an inherent and mundane aspect of new computational systems, means that the new form of governmentality is inevitable, and thus quickly becomes taken–for–granted and seen as mundane or banal in character. Hence, the reason we use the term 'mundane management' (see discussion section).

As detailed, Agre's capture model has utility in thinking through the effects of software on new forms of governmentality. Clearly, the ways in which capta is generated and how it is being used has changed with the use of information systems and the widespread introduction of grammars of action to activities. That said, the surveillance model still persists, particularly in the areas of law enforcement and crime prevention. Moreover, given the drive towards pervasive computing, the capture model is still open to use by states for mass surveillance in ways that (self)–discipline. As illustrated below, this is particularly the case with regards to issues such as national security and the policing of borders, or the delivery of nationalized services such as welfare provision. In many ways then, a new conceptual model is needed that consists of a spectrum — from the traditional surveillance model, little effected by grammars of action, through capture models that are used for traditional–style, statist surveillance, to capture models limited to specific systems. As illustrated below, air travel constitutes a capture–surveillance model that is operated largely by statist institutions, but with cooperation with private business where necessary.

Airport security and immigration

Perhaps the most visible and technologically significant example of the introduction of mundane management is the regulation of national and international air travel. Two different but related issues have helped to transform the regulation of people traveling by air between locations in the last decade. First, growing security fears culminating with the 9/11 attacks has led to a transformation in security procedures. Second, moral panics over illegal immigrants have led to reforms in immigration procedures. In both cases, information systems have become vital pieces of infrastructure, introducing new grammars of action that seek to identify and evaluate the risk and true identity of travelers, and which are supported by a powerful discursive regime that focuses on law enforcement and counter–terrorism, and citizenship and fraud. The systems being developed, we would argue, are examples of our hybridized capture–surveillance model. In America these include the U.S. Visitor and Immigrant Status Indicator Technology (US–VISIT), APIS (Advanced Passenger Information System), and Secure Flight programs. In the U.K., Project Semaphore, the first phase of the e–Borders program [6]. Other systems are being developed and piloted in other countries, such as the Smart Borders in Canada (Canadian Government, 2004). These programs aim to strengthen border controls by identifying and tracking people prior to and as they travel, verifying their departure, and building up a profile of individual movements over time.

The US–VISIT system is operated by the U.S. Department of Homeland Security (DHS) and aims to regulate the flow of people in and out of the U.S. For those needing a visa to travel to America, biometric data (digital finger–scans and photographs) is a key form of capta, collected at the point of application (usually a U.S. Consol office in the country of origin) and checked against a system of interlinked databases for known criminals and suspected terrorists. When the traveler arrives in the U.S. the same biometrics are used to verify that the person is that 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 (European Commission, 2004). The system is being developed and operated by the Accenture–led Smart Border Alliance, through a contract worth up to US$10bn over the next 10 years (Leyden, 2004). At its core, the system will consist 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, 2004a) (see Table 2). The system produced will have a 100–year data retention period and the data contained within will be 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 will be 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 (INA), or other governing orders, treaties or regulations and assisting other Federal agencies to protect national security and carry out other Federal missions.” [7]

This sharing of capta across agencies is problematic in that the capta will potentially be open to use by the 199 data mining programs identified by the General Accounting Office (GAO) in U.S. government departments (Privacy International, 2004) for purposes beyond security and immigration.

Table 2: US–VISIT increment 2 processes and data usage
Source: DHS, 2004a

System/Application	Data In	Data Out
TECS	Passenger manifest, admission data, photo (NIV), visa data (NIV), DocKey	Visa data (NIV), passenger manifest, DocKey (including biographic watch list hit/match), photo (NIV), admission data, audit log
IDENT	DocKey, photo, fingerprints, biographic data (watch list updates)	DocKey (including biometric watch list

		hit/match), fingerprints, audit log
ADIS	Passenger manifest, admission data, DocKey, complete name, DoB, gender, country of birth, nationality, U.S. destination address, visa class, visa number, passport number, country of issuance, SSN18, alien number, I–94 number, POE, entry date, POD, departure date, admission data (current/requested), case status, SEVIS status change date, SEVIS ID (current/requested)	DocKey, complete name, DoB, gender, nationality, visa type, visa number, passport number, country of issuance, POE, entry date, POD, departure date, admission data, SEVIS ID, SEVIS status, status change date, audit log
Workstation	Travel document data, visa data, passenger manifest, DocKey (including biographic and biometric watch list hit/match), photo, fingerprints, admission data, I–94 data	Updated passenger manifest, DocKey, photo, fingerprints, admission data, I–94 data
Departure Device	TBD pending exit pilot Evaluation	TBD pending exit pilot Evaluation
Candidate Verification Tool (CVT)	Candidate & subject fingerprints, FINs, photos, verification history	Verification decision
Secondary Web Tool	Encounter data, FIN (previous encounter)	

US–VISIT is the successor to NSEERS (National Security Entry Exit Registration System) implemented from September 2002 by the Department of Justice (DHS, 2003). NSEERS focused initially on the non–immigrant alien population from designated countries that were deemed to be of risk to national security post 9/11 (Iran, Iraq, Libya, Sudan, Syria, Afghanistan, Algeria, Bahrain, Eritrea, Lebanon, Morocco, North Korea, Oman, Qatar, Somalia, Tunisia, United Arab Emirates, Yemen, Saudi Arabia and Pakistan; UT Watch, 2003) and “others who met a combination of intelligence–based criteria that identified them as a potential security risk.” (DHS, undated) Selection was twofold, with inspectors able to refer any individual, based on national security criteria and intelligence reports, to a detailed examination, and all males born on or before 15 November 1986, required to register at a local district immigration office (including an interview and the collection of fingerprints and a photograph) (Findbiometrics, 2003).

APIS targets suspect or high–risk passengers by checking for matches against a multi–agency database ...

In addition to US–VISIT, passengers on international flights will continue to be pre–screened by U.S. Customs and Border Protection (CBP) using APIS (Advanced Passenger Information System). APIS uses information from the machine–readable part of a passport along with information supplied by air carriers. (This links to other layers, *i.e.*, international standards in the capta ontology of passports determined by U.N. quango ICAO.) APIS requires international air carriers to provide U.S. Customs with “an electronic manifest detailing the name, date of birth, sex, travel document number, and nationality of the document of each passenger and crew member before the aircraft lands in the United States.” (U.S. Customs, 2001) APIS targets suspect or high–risk passengers by checking for matches against a multi–agency 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 (INS), the State Department, and 21 other federal agencies (U.S. Customs, 2001). APIS data is also compiled in the Bureau of Immigration and Customs Enforcement’s (ICE) Arrival and Departure Information System (ADIS) to match arrivals with departures, with information on students forwarded to to the Student and Exchange Visitor Information System (SEVIS) (Findbiometrics, 2003).

In addition to airport screening, as part of the US–VISIT program, the U.S. DHS plans to begin issuing special identification devices to foreign visitors arriving by foot and by car by 31 July 2005 (Gilbert, 2005); tests began in the of 2006 [8]. The devices will contain a RFID (radio frequency identification) chip that uniquely identifies the visitor. Border officials will be able to scan the chips from a distance, with the visitor details broadcast via radio signal. Two other programs include C–TPAT (Customs–Trade Partnership Against Terrorism) (U.S. Customs and Border Protection, undated a), an opt–in scheme where in return for expedited processing at border crossings shippers prove they have strengthened the security of their supply chains, and the Container Screening Initiative (CSI; U.S. Customs and Border Protection, undated b) that identifies and target high–risk containers using intelligence information to identify and target containers that pose a risk for terrorism, and pre–screens containers at the port of departure using technologies such as radiation detectors and large–scale radiographic imaging machines (Rothman, 2004).

US–VISIT is to be complemented the Transportation Security Administration’s (TSA, a division of DHS) “system of systems” approach to security which includes the screening of baggage and passengers, fortified cockpit doors, federal air marshals aboard flights, armed federal flight deck officers and the Secure Flight program (DHS, 2004b). The Secure Flight program monitors internal flights, and accordingly American citizens. Secure Flight is the replacement for the CAPPS (Computer Assisted Passenger Prescreening System) program and is effectively the much–maligned CAPPS II program under a different name — the main differences being that the system will only look for known or suspected terrorists, not other law enforcement violators, that it will include a redress mechanism if passengers believe they have been unfairly or incorrectly selected for additional screening (Sternstein, 2004), and it will not initially have new data requirements for airline reservations, but it will be looking at whether those are necessary [Singel, 2004]). See Table 3 for comparison of the passenger screening systems. That said, while CAPPS II screens an average of 16 percent of air passengers, Secure Flight will, according to the TSA, still screen five or six percent (Sternstein, 2004) and clearly this many passengers are not all known or suspected terrorists.

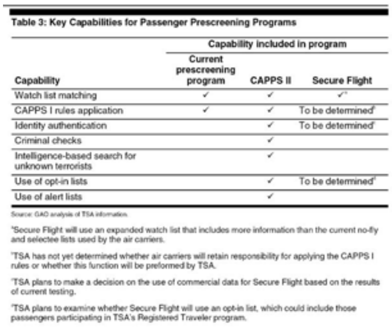

Table 3: Key Capabilities for Passenger Prescreening Programs

	Capability included in program		
Capability	Current prescreening program	CAPPS II	Secure Flight
Watch list matching	✓	✓	✓[a]
CAPPS I rules application	✓	✓	To be determined[b]
Identity authentication		✓	To be determined[c]
Criminal checks		✓	
Intelligence-based search for unknown terrorists		✓	
Use of opt-in lists		✓	To be determined[d]
Use of alert lists		✓	

Source: GAO analysis of TSA information.

[a] Secure Flight will use an expanded watch list that includes more information than the current no-fly and selectee lists used by the air carriers.

[b] TSA has not yet determined whether air carriers will retain responsibility for applying the CAPPS I rules or whether this function will be preformed by TSA.

[c] TSA plans to make a decision on the use of commercial data for Secure Flight based on the results of current testing.

[d] TSA plans to examine whether Secure Flight will use an opt-in list, which could include those passengers participating in TSA's Registered Traveler program.

Under the CAPPS II scheme airlines asked passengers for personal details at the reservation stage, including full name, date of birth, home address, and home telephone number (DHS, 2004b) and used the PNR (Passenger Name Record) generated by booking systems (such as Galileo/Apollo, Sabre, Amadeus and Worldspan) for booking flights, hotels and car hire. A PNR is a record that contains detailed information about an individual's travel that consists of information provided by the passenger at the reservation stage. The PNR varies between booking systems but usually includes a minimum of passenger name, reservation date, travel agency, travel itinerary, form of payment, and flight number. In May 2004, the European Union agreed to 34 field PNRs being transferred to U.S. Customs and Border Protection, including credit card information (Spy Blog, 2004) [see Table 4]. Using this information CAPPS II verified the identity of the passenger and conducted a risk assessment using commercial and government data, and updated the TSA's "Passenger and Aviation Security Screening Records" (PASSR) database (Hasbrouck, undated). The risk assessment resulted in an assigned screening level — no risk, unknown or elevated risk, or high risk. Based on the assigned screening passengers could be detained, interrogated or made subject to additional searches. Importantly, the rules of grammar that lie at the root of these determinations are purposefully secret, being classified "Sensitive Security Information", and as such not open to scrutiny (in terms of independent verification of their effectiveness) or informed challenge (in terms of equity issues, such as racial profiling). CAPPS II was criticized for a failing on normative grounds and replaced due to the ease with 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, 2004c) TSA also acknowledged fear of "mission creep" as a factor.

Table 4: PNR data elements required by U.S. Customs and Border Protection from air carriers

Source: Spy Blog, 2004

1. PNR record locator code
2. Date of reservation
3. Date(s) of intended travel
4. Name
5. Other names on PNR
6. Address
7. All forms of payment information
8. Billing address
9. Contact telephone numbers
10. All travel itinerary for specific PNR
11. Frequent flyer information (limited to miles flown and address(es))
12. Travel agency
13. Travel agent
14. Code share PNR information
15. Travel status of passenger
16. Split/Divided PNR information
17. Email address
18. Ticketing field information
19. General remarks
20. Ticket number
21. Seat number
22. Date of ticket issuance
23. No show history
24. Bag tag numbers
25. Go show information
26. OSI information (Other Supplementary Information)
27. SSI/SSR information Special Service Information/Request (*e.g.* assistance/diet)
28. Received from information
29. All historical changes to the PNR
30. Number of travelers on PNR
31. Seat information
32. One–way tickets
33. Any collected APIS information
34. ATFQ fields (Automatic Ticket Fare Quote)

That said, the Secure Flight program is a scaled back version of CAPPS II not a completely new system and Lockheed Martin Management and Data Systems, the CAPPS II contractors, will develop and operate the Secure Flight program for the TSA. Accordingly, as stated by TSA,

> “Secure Flight will involve the comparison of information in PNRs for domestic flights to names in the Terrorist Screening Database (TSDB) maintained by the Terrorist Screening Center (TSC) [housed by the FBI and presently includes 120,000 names (Singel 2004) [9]], to include the expanded TSA No–Fly and Selectee Lists, in order to identify individuals known or reasonably suspected to be engaged in terrorist activity. TSA will apply, within the Secure Flight system, a streamlined version of the existing CAPPS rule set related to suspicious indicators associated with travel behavior, as identified in passengers’ itinerary–specific PNR.” (DHS, 2004c)

In the test phase, passenger identifying information will be cross–referenced to commercial data held by data aggregators, specifically those who provide services to banking, mortgage and credit industries to check authenticity, accuracy and for anomalies.

It is likely that US–VISIT and Secure Flight will be supplemented by other systems. For example, the TSA are piloting another passenger profiling system, SPOT (Screening of Passengers by Observation Techniques) (Donnelly, 2004). This system aims to use staff to identify suspicious individuals by using the principles of surveillance and detection (rather than by technology alone). Passengers who exhibit unusual or anxious behavior will be identified for extra screening through face–to–face interviews with local police to determine whether any threat exists. If the pilot is successful it will be rolled out to the 429 commercial airports in the U.S. In addition, the U.S. State Department is hoping to move to a system of e–passports (so called “smart passports”) using embedded RFIDs that will store basic data, including the passport holder’s name, date of birth and place of birth, but has enough memory to also store biometric data, including digital fingerprints, photos and iris scans (Gilbert, 2004).

Initially, Project Semaphore will target the six million passengers who travel on so–called “high risk” routes to and from the U.K. It started operation as a 39–month pilot scheme in December 2004. In phase one it will use passenger information supplied by airlines in advance of travel to screen individuals as they enter and leave the U.K., with information being checked against a database of existing passenger name records and assessed in relation to “risk scales” to identify security risks (Best, 2005). In early February 2005, the Home Office also announced that all visa applicants will be fingerprinted once they arrive at U.K. ports of entry. Further, Project IRIS (Iris Recognition Immigration System), will be piloted from February 2005 at Heathrow. IRIS aims to speed up the admission of pre–assessed *bona fide* travelers, through iris scanning technology, and is due be fully operational by the summer of 2005 (U.K. Home Office, 2004). Enrollment will be voluntary and those accepted into the program will have their eyes filmed using a standard video camera to capture their iris patterns, this being checked in a special fast–track lane at airports to verify personal identification (McCue, 2004). Similar systems are being piloted elsewhere in Europe (Sharma, 2004). It is envisaged that by 2008 the e–Borders program will record all movement into and out of Britain and provide a “comprehensive passenger movement audit trail”. (Besides passenger tracking, the U.K. government is also pushing forward with controversial legislation for national ID card and database based on biometric technology.)

Taken together these systems aim to create a dossier of travel for individuals that last a lifetime.

Taken together these systems aim to create a dossier of travel for individuals that last 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. Moreover, these systems are representative of the capture model wherein the mechanisms of work are also the techniques of surveillance, but they retain the utility of statist, mass surveillance (hence our notion of a hybrid capture–surveillance model). Here, the grammars of action are the formalized rules of assessment at the heart of the systems (US–VISIT, APIS, Secure Flight) with biographic and biometric capta the basic ontology. Clearly these systems actively shape, both implicitly and explicitly, the nature and procedures of travel (rather than simply surveying). In explicit terms, travelers have to acquire new machine–readable passports, submit to biometric capta generation, and 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. Moreover, the databases, criteria, mechanisms and algorithms underpinning the screening people are impenetrable except for those in control.

Discussion

Even from a cursory analysis such as presented in this paper it should be clear that capture–surveillance systems raise a number of questions concerning the changing nature of governmentality, the implications of these changes, and how the transformations taking place should be theorized. So far, we have outlined a number of new systems with regards air travel and suggested that the transformations taking place are best understood though the notion of a hybrid capture–surveillance system embedded in. In this section, we examine in brief some of the shortcomings of these new systems, and how despite concerns and fallibilities they retain hegemonic status through the implementation of mundane management.

In April 2004, The American Civil Liberties Union (ACLU) published a list of seven reasons to question the integrity and employment of passenger screening and profiling systems. These reasons focused on errors, due process, cost and impact. First, the ACLU suggest, and as the literature makes clear, that capture–surveillance 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 typos, non–updates (*e.g.*, change of address), missing or misleading fields; and, mismatching errors, especially based on names. These errors are especially prevalent in commercial databases sometimes used in profiling systems. Biometric errors include the Failure To Enroll Rate (FTER), wherein the biometric is either unrecognizable or not of a sufficiently high standard (*e.g.*, worn fingerprints), a False Non–Match Rate (FNMR), wherein a subsequent reading does not properly match the enrolled biometric (*e.g.*, face aging), and false positives, wherein a system is so large that there are many near matches leading to people being falsely identified. The ACLU report that with a 99.9 percent accuracy rate there will errors with respect to one million transactions and approximately 100,000 travelers. The TSA are predicting an error rate of at least four percent error (or four million people) seriously undermining the effectiveness and integrity of the system.

Second, with respect to due process, the ACLU points out that travelers will be judged largely in secret with the findings non–disclosed, and moreover there will be a limited process of notification, correction and appeal. Third, the ACLU suggests that the new systems place an unnecessary burden on airlines, travel agents and the public by passing the costs for a flawed and suspect system onto them. Fourth, the ACLU identifies three negative impacts with respect to individuals: privacy infringement through the creation of lifetime travel dossiers; potential discriminatory impact by fostering systematic unequal treatment (*e.g.*, the so–called "flying while Arab" effect where those of Arab descent are subject to extra screening and profile based simply on race and ethnicity); and, the potential for control creep.

... travelers will be judged largely in secret with the findings non–disclosed, and moreover there will be a limited process of notification, correction and appeal.

Control creep occurs when "social control apparatus progressively expands and penetrates (or 'creeps') into different social arenas, in response to a set of inchoate fears about a sense of security in late–modernity." [10] This control creep can happen in at least three ways (ACLU, 2004). First, more and more capta is generated in an effort to be exhaustive and comprehensive in profiling. Second, capta becomes used for purposes different to those it was generated for. Third, the system is extended to other social arenas. In other words, technologies designed to identify, monitor and regulate one set of people (*e.g.*, terrorists) in one kind of social space (*e.g.* airports) are expanded in scope to other social arenas (such as flagging so–called "dead–beat dads" who fail to make child support payments). For example, airport security measures are extended to other forms of public transport, are used to "protect" national monuments, and employed to monitor flows of traffic and goods on highways and through ports, and are used to identify criminals, defaulters, etc. Such extensions raises a number of fears with respect to civil liberties and privacy infringement, social sorting, and the limiting of social freedoms on the basis of religious and cultural identities (Graham and Wood, 2003; Lyon, 2003). That is, these systems and their capta will not simply be used to ensure safe and secure travel, but will be applied to other aspects of life in ways hidden to individuals yet actively shaping their worlds (including discriminatory effects, limiting their ability to travel, their access to certain services and goods, making it easier for business to enact differential pricing schemes, and so on).

Given the potential for capture errors, flaws in procedures and structures, and potential impacts and misuses of the systems there has, to date, been remarkably little mass, organized resistance to new capture–surveillance systems by either individuals, political lobby groups or other states. The resistance that has occurred is either expressed in disquiet, individual resistances such as boycotts of travel to particular destinations, or legal challenges to state policy by groups such as the ACLU. These resistances, however, are a long way short of a tipping point wherein resistance becomes so great that it starts to undermine the system and places pressure on governments, airports and airlines to modify or abandon systems. Revisiting our earlier discussion, we posit that this lack of overt, organized resistance is due to five reasons that instill measures of self–disciplining and work to maintain the new hegemonic formation.

First, people have been persuaded to the new emerging logic either through disciplining or seduction. In this context, advances in surveillance technologies and systems are seen as necessary to: ensure safety and security in an unstable world, particularly in relation to the so–called “war on terror”; police immigration and issues of citizenship given moral panics surrounding “illegal” immigrants and asylum seekers; and, reduce costs and increase the economic competitiveness and productivity of airlines and airports. In the case of U.S., the DHS, and in the U.K., the Home Office, have mobilized discourses of safety, security, efficiency, anti–fraud, and citizenship, at the same time continuing to warn of imminent terrorist threat and the dangers of (illegal) immigrants, in order to justify and legitimate mundane governmentality. For example, in the Project Semaphore press release U.K. 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.” (U.K. Home Office, 2004)

DHS similarly argues that these systems will produce consistency and fairness, while at the same time reducing costs and efficiency:

> “Secure Flight will automate the vast majority of watch list comparisons; will allow TSA to apply more consistent procedures where automated resolution of potential matches is not possible; and will allow for more consistent response procedures at airports for those passengers identified as potential matches. ... It will dramatically improve the administration of comparisons of passenger information with data maintained by TSC and will reduce the long–term costs to air carriers and passengers associated with maintaining the present system, which is operated individually by each air carrier that flies in the United States.” (DHS, 2004c)

Second, people see the changes that are occurring as simply an extension of previous systems, which they are already conditioned to. In other words, most people do not see the introduction of biometrics as a step change in the levels and sophistication of surveillance, particularly in an environment that has long been subject to levels of surveillance in excess of nearly any other space. Rather, new technologies and systems are seen as the outcome of an inevitable progression as new developments occur. This viewpoint is supported by marketing and lobbying efforts on the part of IT vendors and technology consultants.

Third, given this progression, the new grammars of action enacted and how surveillance is structured and used is seen as an inherent, and therefore unchallengeable, aspect of the system. That is, the system is necessarily built in a certain way, with certain parameters, thus grammars of action are hard–coded into the make-up of the system in a “natural”, “neutral” way (that’s the way it had to be to fulfill certain requirements such as safety and security targets), rather than the system and its parameters being seen as something that are relational and contingent in their formulation, design and implementation.

Fourth, the point of contact for most travelers is relatively painless — a few security questions, a swipe of a passport, a finger on a scanner plate — with the bulk of screening taking place in the background and unbeknownst to them. In this sense, while being subject to new capture modes of surveillance, this exposure is seemingly benign and routine rather than invasive.

... the nature of the surveillance system works to instill a deep level of reflexive self–disciplining.

Fifth, we believe that many people do not openly resist new capture–surveillance systems because they are worried of the consequences protest. The fear in these cases is one of mistreatment when traveling (such as extra security checks and delays) or blacklisting from certain travel all together (for example, being barred entry to a country). Here, the nature of the surveillance system works to instill a deep level of reflexive self–disciplining. That is, individuals are wary of new systems fearing potential misuse and abuse but feel powerless to openly challenge the system for fear of inciting those potential misuses and abuses. There is a certain logic to these fears given the “cold”, officious treatment by security personnel and immigration officers and stories circulating in the news media and individual networks of mistreatment when traveling. These stories are either dismissed by officials as false or hearsay or portrayed as inevitable, “minor” and rare misunderstandings and the price of secure and safe travel. In other words, stories are undermined in order to reassert the operating doxa.

Programs such as Project Semaphore and Secure Flight then are multifaceted, used for different purposes — the fight against illegal immigrants and fraud, to ensure law enforcement and counter–terrorism measures, to improve efficiency and reduce costs for both the state and the airline industry. At the same time these programs argue that they minimize hassle for low–risk passengers. As such they are cross–justified, playing on peoples’ fears and prejudices, travelers’ and airlines’ annoyance at inefficiencies and waste, and arguing that if you have nothing to hide, you have nothing to fear. As a result, taken together the five reasons outlined have led to the almost *carte blanche* development of new capture–surveillance systems, with associated legislation and systems of government.

Conclusion

In this paper we have sought to outline the ways in which the use of software and information systems has transformed the monitoring, registration and regulation of air travelers introducing a new mode of governmentality that we have termed mundane management. In short, software has led to a step–change in the form and scope of surveillance technologies employed by airports and airlines for screening and profiling passengers. These changes are supported by a powerful discursive regime that employs seductive discourses of safety, security, anti–fraud, citizenship, competitiveness and productivity and which works to silence resistance.

Recent literatures have tended to use a Foucaultian model to understand the nature of air travel surveillance. We are sympathetic to this position, but believe it more productive to re–think this model with respect to Agre’s capture model. The resulting capture–surveillance model recognizes that the employment of software systems in the various tasks that constitute air travel (booking flights, checking in, security checks, immigration, etc.) means that the processing and monitoring of passengers has become highly formalized through grammars of action utilizing highly specific biographical and biometric capta throughout the air travel assemblage. Consequently, capture has become an integral part of air travel, actively reshaping how an activity is undertaken, rather than simply working to discipline behavior. Further these systems, in contrast to Foucault’s observations about surveillance being openly visible (and this is its power to discipline), are largely hidden and covert in operation. In the case of air travel they are also, contra to Agre’s capture thesis, centralized and statist in nature.

Paradoxically, these systems have significant implications to civil liberties and privacy, especially through control creep, and yet are ambivalently accepted. In this sense they constitute a form of mundane management that has quickly become banal in its operation and thus hegemonic in status. As noted in the previous section, the lack of resistance to systems that have very significant powers of screening, profiling and disciplining is, we believe, the result of how the systems have been "sold" to the public through a discursive regime that portrays the resulting systems as having numerous positive effects and is technologically inevitable, but also works to silence dissent through potential threats to civil liberties.

While we have focused on air travel in this paper, it should be noted that systems of capture–surveillance are being developed with respect to other domains such as automobiles (Dodge and Kitchin, forthcoming). Again, while driving and vehicles have long been subject to regulation and surveillance, a plethora of new location–based, dynamic capture–surveillance technologies are being developed and publicly and commercially implemented. For example, cars are increasingly being fitted with software systems that not only monitor and mediate the engine and other systems but also record the driver's driving; GPS–based navigation and tracking systems are being used by car rental and anti–theft companies monitor the real–time location of a vehicle to the nearest few meters; a range of "smart" media have been added to road infrastructure including speed, red light and lane camera systems using telematic networks and automatically tolling systems.

In many ways, these systems raise more worrying questions and concerns given they are being applied to a much more common, fluid and diverse aspect of daily life and therefore have the potential to develop in unanticipated ways creating new forms of governmentality. Whereas air–travel capture–surveillance system are statist and explicitly built to monitor and control along well–defined lines, automobile systems are being designed and built for diverse purposes, often being used for purposes beyond their initial intention (*e.g.*, navigational aids in rental cars being used to track renters movements and to impose misuse fines — driving out of state or off–road; or parents tracking a child driver's movements), and are being developed and operated by multiple agencies including the state and its agencies, car manufacturers, rental car companies, and other third parties. As such, while more research is needed to tease out the changing regulatory nature of air travel, there is perhaps a more pressing need to examine capture–surveillance systems in all their forms across multiple domains and their effects v*vis–à–vis* governmentality.

About the authors

Rob Kitchin is Professor of Human Geography and Director of the National Institute for Regional and Spatial Analysis at the National University of Ireland–Maynooth. He is the managing editor of the journal *Social and Cultural Geography*, co–editor–in–chief of the *International Encyclopedia in Human Geography*, author of *Cyberspace: The World in Wires* (Wiley, 1998), and co–author or co–editor of numerous other volumes.
Web: www.nuim.ie/staff/rkitchin
E–mail: Rob [dot] Kitchin [at] nuim [dot] ie

Martin Dodge is a lecturer in the School of Environment and Development, University of Manchester, and runs the Cybergeography project including the *Atlas of Cyberspace*.
Web: www.cybergeography.org/
E–mail: m [dot] dodge [at] manchester [dot] ac [dot] uk

Notes

1. Jensen (cited in Becker, 1952) details that capta are units of data that have been selected and harvested from the sum of all potential data. Here, *data* (derived from the Latin *dare*, meaning 'to give') is the total sum of facts that an entity can potentially 'give' to government or business or whomever is constructing a database. Capta (derived from the Latin *capere*, meaning 'to take') are those facts that those constructing the database decide to 'take' given that they cannot record or store everything.

2. Agre, 1994, p. 754.

3. Wardrip–Fruin, 2003, p. 757.

4. Agre, 1994, p. 752.

5. Wardrip–Fruin, 2003, p. 757.

6. A cross–cutting initiative co–ordinated by the Home Office in partnership with key border control, law enforcement and intelligence agencies.

7. *Federal Register*, 2003, cited in Privacy International, 2004.

8. U.S. Department of Homeland Security, 2005. "Testing of radio frequency identification (RFID) technology at land borders questions and answers," Press release, at http://www.dhs.gov, accessed 20 August 2006.

9. This figure is suspiciously the same as that generated by the Multistate Anti–TeRrorism Information eXchange (MATRIX) programme. This system combines information from government databases and private–sector data companies about individuals, and makes that data available for search by government officials. After 9/11 this system was used to identify, by calculating "terrorist quotient" suspected terrorists residing in the U.S. Some 120,000 individuals fitted the "characteristics" of a terrorist.

10. Innes, 2001, no pagination.

References

P.E. Agre, 1994. “Surveillance and capture: Two models of privacy,” *Information Society*, volume 10, number 2, pp. 101–127. Reprinted In: N. Wardrip–Fruin and N. Montfort (editors), 2003. *The NewMediaReader*. Cambridge, Mass.: MIT Press.

L. Althusser, 1971. *Lenin and philosophy, and other essays*. Translated from the French by B. Brewster. London: New Left Books.

American Civil Liberties Union (ACLU), 2004. “The seven problems with CAPPS II,” at http://www.aclu.org/Privacy/Privacy.cfm?ID=15426&c=130, accessed 20 August 2006.

H. Becker, 1952. “Science, culture, and society,” *Philosophy of Science*, volume 19, number 4, pp. 273–287.

J. Best, 2005. “Fingerprints, iris recognition and tagging ‘to cut immigration’,” at http://software.silicon.com/security/0,39024655,39127657,00.htm, accessed 20 August 2006.

Canadian Government, 2004. “Securing an open society: Canada’s national security policy,” http://www.forces.gc.ca/site/newsroom/view_news_e.asp?id=1363, accessed 20 August 2006.

M. Dodge and R. Kitchin, forthcoming. “The automatic management of drivers and driving spaces,” *Geoforum* in press.

M. Dodge and R. Kitchin, 2005. “Codes of life: Identification codes and the machine–readable world,” *Environment and Planning D: Society and Space*, volume 23, number 6, pp. 851–881.

M. Dodge and R. Kitchin, 2004. “Flying through code/space: The real virtuality of air travel,” *Environment and Planning A*, volume 36, number 2, pp. 195–211.

S.B. Donnelly, 2004. “Spotting the airline terror threat,” *Time* (2 October), at http://www.time.com/time/nation/article/0,8599,708924,00.html, accessed 20 August 2006.

European Commission. Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens (IDABC), 2004. “INT: US Administration extends US–VISIT programme to visa waiver countries,” (5 April), at http://europa.eu.int/idabc/en/document/2382/348, accessed 20 August 2006.

Federal Register, 2003. “Department of Homeland Security [DHS/ICE–CBP–CIS–001] Privacy Act of 1974; System of Records,” *Federal Register*, volume 68, number 239 (12 December), and at http://www.privacyinternational.org/issues/terrorism/library/USVISITfederalregister03-30761.pdf, accessed 20 August 2006.

Findbiometrics, 2003. “Fact Sheet: US–VISIT Program — October 30, 2003,” http://www.findbiometrics.com/viewnews.php?id=587, accessed 20 August 2006.

M. Foucault, 1978. *The history of sexuality*, volume one. New York: Pantheon Books.

M. Foucault, 1976. *Discipline and punish: The birth of the prison*. London: Allen Lane.

A. Gilbert, 2005. "States to test ID chips on foreign visitors," *CNET News.com* (26 January), at http://news.com.com/States+to+test+ID+chips+on+foreign+visitors/2100-1039_3-5552120.html, accessed 20 August 2006.

A. Gilbert, 2004. "U.S. moves closer to e–passports," *CNET News.com* (25 October), at http://news.com.com/U.S.+moves+closer+to+e-passports/2100-1012_3-5425314.html, accessed 20 August 2006.

S. Graham and D. Wood, 2003. "Digitising surveillance: Categorisation, space and inequality," *Critical Social Policy*, volume 23, pp. 227–248.

E. Hasbrouck, undated. "What's in a Passenger Name Record (PNR)?" http://hasbrouck.org/articles/PNR.html, accessed 20 August 2006.

E. Higgs E, 2001. "The rise of the information state: The development of central state surveillance of the citizen in England, 1500–2000," *Journal of Historical Sociology*, volume 14, number 2, pp. 175–197.

M. Innes, 2001. "Control creep," *Sociological Research Online*, volume 6, number 3, at http://www.socresonline.org.uk/6/3/innes.html, accessed 20 August 2006.

J. Leyden, 2004. "Accenture wins $10bn homeland security gig," *The Register* (2 June), at http://www.theregister.co.uk/2004/06/02/accenture_homeland_security_win/, accessed 20 August 2006.

D. Lyon, 2003. "Surveillance as social sorting: Computer codes and mobile bodies," In: D. Lyon (editor). *Surveillance as social sorting: Privacy, risk, and digital discrimination*. London: Routledge, pp. 13–30.

A. McCue, 2004. "Iris recognition to be installed across UK airports," *Silicon.com* (15 June), at http://software.silicon.com/security/0,39024655,39121368,00.htm, accessed 20 August 2006.

Privacy International, 2004. "The Enhanced U.S. Border Surveillance System. An Assessment of the Implications of US VISIT," at http://www.privacyinternational.org/issues/terrorism/rpt/dangers_of_visit.pdf, accessed 20 August 2006.

P. Rothman, 2004. "Technology on the line,," *Government Security* (1 April), http://govtsecurity.com/mag/technology_line/, accessed 20 August 2006.

D.C. Sharma, 2004. "Protecting your ID: German airport begins biometric checking Lufthansa chooses iris scanning over other options," *Silicon.com* (16 February), at http://www.silicon.com/research/specialreports/protectingid/0,3800002220,39118396,00.htm, accessed 20 August 2006.

R. Singel, 2004. “Secure flight gets wary welcome,” *Wired News* (27 August), at http://www.wired.com/news/privacy/0,1848,64748,00.html, accessed 20 August 2006.

Spy Blog, 2004. “EU Commission betrays Passenger Name Record data privacy to USA despite EU Parliament” (31 May), at http://www.spy.org.uk/spyblog/2004/05/eu_commission_betrays_passenge.html, accessed 20 August 2006.

A. Sternstein, 2004. “TSA launches Secure Flight” (27 August), at http://www.fcw.com/fcw/articles/2004/0823/web-tsa-08-27-04.asp, accessed 20 August 2006.

U.K. Home Office, 2004. “Cutting–edge technology to secure UK borders for 21st century,” at http://www.gnn.gov.uk/content/detail.asp?NewsAreaID=2&ReleaseID=130801, accessed 20 August 2006.

U.S. Customs, 2001. “New law makes APIS a must For international air carriers,” at http://www.cbp.gov/xp/CustomsToday/2001/December/custoday_apis.xml, accessed 20 August 2006.

U.S. Customs and Border Protection, undated a. “C–TPAT fact sheet and frequently asked questions,” at http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/ctpat_faq.xml, accessed 20 August 2006.

U.S. Customs and Border Protection, undated b. “CSI in brief” (15 February), at http://www.cbp.gov/xp/cgov/border_security/international_activities/csi/csi_in_brief.xml, accessed 20 August 2006.

U.S. Department of Homeland Security (DHS), undated. “US–VISIT FAQs: NSEERS and US–VISIT,” http://www.dhs.gov/dhspublic/display?theme=91&content=4095.

U.S. Department of Homeland Security, 2004a. “US–VISIT Program, Increment 2, Privacy Impact Assessment,” (14 September), at http://www.dhs.gov/interweb/assetlibrary/US-VISIT_PIA_09142004.pdf, accessed 20 August 2006.

U.S. Department of Homeland Security, 2004b. “Fact sheet: CAPPS II at a glance,” at http://www.dhs.gov/dhspublic/display?content=3162, accessed 20 August 2006.

U.S. Department of Homeland Security, 2004c. “Transport Security Administration. Privacy Impact Assessment. Secure Flight Test Phase,” (TSA–2004–19160), http://www.tsa.gov/interweb/assetlibrary/Secure_Flight_PIA_Notice_9.21.04.pdf.

U.S. Department of Homeland Security, 2003. “US–VISIT Program, Increment 1 Privacy Impact Assessment Executive Summary,” (18 December), at http://www.dhs.gov/interweb/assetlibrary/VISITPIAfinalexecsum3.pdf, accessed 20 August 2006.

U.S. General Accounting Office (GAO), 2005. “Secure flight development and testing under way, but risks should be managed as system is further developed” (GAO–05–356), at http://www.gao.gov/new.items/d05356.pdf, accessed 20 August 2006.

UT Watch, 2003. “Special registration under NSEERS” (7 January), at http://www.utwatch.org/security/nseers.html, accessed 20 August 2006.

N. Wardrip–Fruin, 2003. “Introduction to surveillance and capture: Two models of privacy,” In: N. Wardrip–Fruin and N. Montfort (editors). *The NewMediaReader*. Cambridge, Mass.: MIT Press, pp. 737–739.

Editorial history

Paper received 15 August 2006; accepted 25 August 2006.

Contents Index

Software and the mundane management of air travel by Rob Kitchin and Martin Dodge
First Monday, special issue number 7 (September 2006),
URL: http://firstmonday.org/issues/special11_9/kitchin/index.html