Durham University

Durham Research Online

Deposited in DRO:

03 May 2011

Version of attached file:

Accepted Version

Peer-review status of attached file:

Peer-reviewed

Citation for published item:

Amoore, L. (2009) 'Algorithmic war : everyday geographies of the war on terror.', Antipode., 41 (1). pp. 49-69.

Further information on publisher's website:

http://dx.doi.org/10.1111/j.1467-8330.2008.00655.x

Publisher's copyright statement:

The definitive version is available at www.interscience.wiley.com

Additional information:

Use policy

The full-text may be used and/or reproduced, and given to third parties in any format or medium, without prior permission or charge, for personal research or study, educational, or not-for-profit purposes provided that:

- a full bibliographic reference is made to the original source
- a link is made to the metadata record in DRO
- the full-text is not changed in any way

The full-text must not be sold in any format or medium without the formal permission of the copyright holders.

Please consult the full DRO policy for further details.

Durham University Library, Stockton Road, Durham DH1 3LY, United Kingdom
Tel : +44 (0)191 334 3042 | Fax : +44 (0)191 334 2971
https://dro.dur.ac.uk

Algorithmic War: Everyday Geographies of the War on Terror

Louise Amoore

Department of Geography
University of Durham
South Road
Durham DH1 3LE
UK

louise.amoore@durham.ac.uk
tel: 00 (+44) 0191 334 1969
fax: 00 (+44) 0191 334 1801

Abstract

Technologies that deploy algorithmic calculation are becoming ubiquitous to the homeland securitization of the war on terror. From the surveillance networks of the city subway to the biometric identifiers of new forms of border control, the possibility to identify 'association rules' between people, places, objects and events has brought the logic of pre-emption into the most mundane and prosaic spaces. Yet, it is not the case that the turn to algorithmic calculation simply *militarizes* society, nor even that we are witnessing strictly a *commercialization* of security. Rather, algorithmic war is one form of Foucault's sense of a "continuation of war by other means", where the war-like architectures of self/other, here/there, safe/risky, normal/suspicious are played out in the politics of daily life. This paper explores the situated interplay of algorithmic practices across commercial, security, and military spheres, revealing the violent geographies that are concealed in the glossy techno-science of algorithmic calculation.

Algorithmic War: Everyday Geographies of the War on Terror

> In the search for terrorists and terrorist cells, we are employing predictive technology that was previously utilized by the business community.
>
> (US Department of Justice 2002).

> The final decision can come only from war.
>
> (Foucault 2003 [1976]: 16).

In 2005, the then US Secretary of Homeland Security, Tom Ridge, and the under Secretary Asa Hutchinson, resigned their government positions and established businesses supplying expert systems in the burgeoning homeland security market. Ridge, having taken a directorship of *Savi Technology*, a radio frequency identification (RFID) technology company, founded *Ridge Global LLC*, a consulting firm specializing in domestic security and crisis risk management (*New York Times* 2006: 34). By 2006, when RFID had become a primary security technology proposed for passports, visas, and transportation systems, Ridge had been appointed government applications consultant for *Deloitte and Touche*'s RFID services. Hutchinson, for his part, established the eponymous *Hutchinson Group*, a homeland security consulting company, and held stocks in *Fortress America Acquisition Corp*, a company trading in the public procurement of private security technologies.

As key figures in an administration that authorized algorithmic computing applications, biometrics, risk management systems and surveillance technologies to help fight the 'war on terror', their move to the private commercial world illustrates an emerging geography of securitization in everyday life. From the remote sensing of bodies on a railway platform, to the securing of identity via biometric algorithms, or the profiling of risk at the airport, the practices of the war on terror exceed any clear distinction between military/civil/commercial spheres. It is not that algorithmic techniques have their origins strictly in the military domain (though as we will see many of them do), nor that society is strictly undergoing renewed *militarization*, but that security practices oscillate back and

forth across different domains. There is, as William Connolly describes it, an emerging "resonance" between security activities:

> Airport surveillance, internet filters, passport tracking devices, legal detention without criminal charges, security internment camps, secret trials, "free speech zones", DNA profiles, border walls and fences, erosion of the line between internal security and external military action – these security activities resonate together, engendering a national security machine that pushes numerous issues outside the range of legitimate dissent and mobilizes the populace to support new security and surveillance practices against underspecified enemies.
>
> (Connolly 2005: 54).

Neither a militarization of society, nor even a commercialization of security, then, what we are seeing is a stitching together of the mundane and prosaic calculations of business, the security decisions authorized by the state, and the mobilized vigilance of a fearful public. It is important to stress here that questioning the logic of militarization is not to underplay the acute violence inherent to this different kind of war. What I call here 'algorithmic war' is one specific appearance of Foucault's Clausewitzian inversion – the "continuation of war by other means", its appeal to technology and expertise rendering the violent force of war somewhat ordinary and invisible (1976/2003: 16). "The role of political power", writes Foucault, "is perpetually to use a sort of silent war to reinscribe the relationship of force, and to reinscribe it in institutions, economic inequalities, language, and even the bodies of individuals" (16-17). Understood in this way, the political practices of homeland security – what Derek Gregory and Alan Pred call "expert solutions" (2007: 1) – are actually sanctioning and reproducing the war-like relations of power seen in the overtly militarized spaces of Afghanistan and Iraq. They target individual bodies, designate communities as dangerous or risky, delineate safe zones from targeted locations, invoke the pre-emptive strike on the city streets.

Algorithmic security is war-like, then, not primarily because it brings military force into closer proximity with our daily commute or airport check-in queue (though of course it

does do this), but because it functions through a war-like architecture. It deploys an "architecture of enmity", a drawing of the lines between self/other; us/them; safe/risky; inside/outside, that makes going to war possible (Shapiro 1997). Though political geography has given critical attention to the performativity of the violent imagination of threat, this has most commonly focused on spaces where the presence of war is visceral and visible – where uniformed military personnel are present of the city streets (Katz 2007); when urban spaces are the targeted sites of war (Graham 2004); or in the tangible violences of Abu Ghraib and Guantanamo Bay (Minca 2005). In this paper, I explore the less visible spaces where the architecture of enmity is present in the form of algorithmic war. In the first section, I trace an extended example of algorithmic calculations deployed to identify 'hidden' associations between people, groups, behaviours and transactions. Initially developed to allow commercial retail players to take strategic decisions in an uncertain future marketplace, algorithmic 'rules of association' have become the basis for pre-emptive state security decisions. In the second section, I focus on the spatiality of algorithmic war, arguing that it has a geography of locatability. Discussing the homeland security applications of radio frequency identification (RFID) technologies, I suggest that the dispersed and diffuse locations of the supply chain (offshore, export processing, control from a distance) are incorporated into state border controls (RFID passports and visas, tracking technologies in public space). Algorithmic war appears to make it possible for the imagination of an open global economy of mobile people, objects and monies, to be reconciled with the post 9/11 rendering of a securitized nation-state.

Probability/Security: Algorithms at the Checkout and in the Subway

In the immediate aftermath of 9/11, the homeland face of the war on terror identified an enemy whose probable future actions were already visible in the traces of life left in existing data. Giving evidence at a US Congressional hearing only five months after 9/11, IBM's federal business manager testified that "in this war, our enemies are hiding in open and available information across a spectrum of databases" (Intelligent Enterprise 2002: 8). Technology consultants and IT providers such as IBM have made the generation of

probabilistic association rules the forefront of homeland security practices. The idea is that locating regularities in large and disparate patterns of data can enable associations to be established between apparently 'suspicious' people, places, financial transactions, cargo shipments and so on (Amoore and de Goede 2005; Ericson 2007). Rules of association are produced by algorithms – models or "decision trees" for a calculation (Quinlan 1986). In effect, algorithms appear to make it possible to translate *probable* associations between people or objects into *actionable* security decisions. In 2003, for example, a US joint inquiry concluded that "on September 11, enough relevant data was resident in existing databases", so that "had the dots been connected", the events could have been "exposed and stopped" (2003: 14). It is precisely this 'connecting of dots' that is the work of the algorithm. By connecting the dots of probabilistic associations, the algorithm becomes a means of foreseeing or anticipating a course of events yet to take place:

> If we learned anything from September 11 2001, it is that we need to be better at *connecting the dots* of terrorist-related information. After September 11, we used credit card and telephone records to identify those linked with the hijackers. But wouldn't it be better to identify such connections before a hijacker boards a plane?
>
> (US Secretary of Homeland Security, Michael Chertoff 2006).

The algorithm appears to make possible the conversion of ex post facto evidence in the war on terror into a judgement made in advance of the event. The significant point here is that probabilistic knowledge, based on the databased residue of daily life, becomes a means of securitization. As the US Inspector General concluded in his survey of government applications of algorithmic techniques, "association does not imply a direct causal connection", but instead it "uncovers, interprets and displays relationships between persons, places and events" (Department of Homeland Security 2006: 10). It is the specific visualization of threat, then, that marks out the algorithm as a distinctive mode of calculation – to be displayed on the screens of border guards, stored on subway travel cards, shared between multiple public and private agencies. In this sense, the algorithm

produces a screened geography of suspicion, on the basis of which 'other' people are intercepted, detained, stopped and searched (Amoore 2007).

How has it become possible, then, for the algorithmic rules of association to become the basis for everyday securitization in the war on terror? In one sense the algorithmic mining of data on the population within the war on terror is but one specific turn in a long history of incorporating uncertainty into calculations via statistics, what Ian Hacking (1990) has called the "taming of chance". Yet, it is in the more prosaic recent histories of probabilistic knowledge in the commercial sphere that algorithmic logics have really begun to define the management of uncertain futures of many kinds – from flood risk in the insurance industry to catastrophe risk in the financial markets (Baker 2002). One particular resonance between the mathematical sciences and commercial worlds is especially worthy of discussion for its subsequent role in processes of securitization. In the summer of 1992, *IBM* research fellow Rakesh Agrawal met for lunch with a senior executive of UK retailers *Marks & Spencer* (*M&S*). Working on mathematical models for locating associations between items in "accumulated data" at the *IBM-Almaden* research centre, Agrawal proposed that *M&S*'s vast data on daily transactions could be used to take strategic corporate decisions. The research paper that resulted from the *IBM-M&S* meeting, and from subsequent work with US retailer *Wal-Mart*, has become the world's most cited work on commercial algorithmic techniques for data mining (Agrawal, Imielinski and Swami 1993).

Let us pause here and briefly reflect on the logic of Agrawal's algorithmic model. "Consider a supermarket with a large collection of items", he writes, "typical business decisions might include what to put on sale, how to design coupons, how to place merchandise on shelves in order to maximize profit" (Agrawal, Imielinski and Swami 1993: 207). Progress in bar-code technology, the research finds, has made it possible to screen transactions "for association rules between sets of items" and "to present an efficient algorithm for that purpose" (1993: 207). Agrawal's examples of commercial questions that the algorithm could model include such prosaic queries as: What pattern of purchases is associated with Diet Coke?; What pattern of items has to be sold with

sausages in order for it to be likely that mustard will also be sold? What proportion of transactions that include bread and butter also include milk? The deployment of algorithmic calculations in this context signals an important move – from the effort to predict future trends on the basis of fixed statistical data to a means of pre-empting the future, drawing probable futures into imminent and immediate commercial decision.

The *IBM* work on association rules in the mathematical and computer sciences, though it achieved ubiquity by 'connecting the dots' in prosaic settings and everyday transactions, significantly established a way of thinking about taking security decisions in the face of an uncertain future. By 2004, Agrawal and his *IBM* team were leading the export of commercial algorithmic techniques to the security sphere, presenting the possibilities of association rules for the "mathematical sciences role in homeland security" (BMSA 2004). The promise that algorithmic calculations held out to the commercial authorities of the 1990s – to enable surveillance from a distance, to make market judgements in advance, to generate patterns of normal and atypical consumer behaviour – is now being re-made in the context of state security desires. At the time of writing *IBM* currently have the software contracts for the Heathrow airport 'MiSense' biometrics system, the UK e-borders 'Iris' and 'Semaphore' trials, and the US biometric borders programme (DHS 2005; Computing 2004; 1). As the logics of commercial data mining cross into security spheres, association rules become a form of 'guilt by association', within which risky bodies, transactions, mobilities are designated and identified.

The decisions taken on the back of algorithmic calculations – detention at international borders (Sparke 2006), freezing of financial assets and targeting of migrant remittances (de Goede 2003; Aitken 2006), interception of cargo at ports (Chalfin 2004) – conceal political difficulty, even discrimination and violence, within an apparently neutral and glossy techno-science. Thus, for example, the algorithmic technologies of the US VISIT 'smart borders' programme, promise to make the "border guard the last line of defense, not the first, in identifying potential threats" (Accenture digital forum 2004: 4; see Amoore 2006). Because the identification of risk is assumed to be already present within the calculation, the border guard is somehow taken off the 'front line'. The screened

appearance of a security threat, then, is always already calculated by the algorithmic performance of association rules – was the ticket paid in cash?; what is the past pattern of travel?; is this a frequent flier?; what in-flight meal was ordered?[1] The risk flag that appears on the border guard's screen is the result of a calculation, itself made on the basis of prior judgments about norm and deviation from norm.

Of course, in one sense there is nothing at all novel in the co-authorization of security decisions by the mathematical and computing sciences, the military and the state (Edwards 1996; Light 2003; Martin 2003). Indeed, a reading of Jenny Edkins' study of the physicists Werner Heisenberg and Niels Bohr suggests historical parallels between the "uncertainty principle in physics", the "cosmology that made the atomic bomb possible", and the "interpretation of human actions" (2003b: 363/369). Put simply, the rejection of causality by quantum physics (embodied also in Agrawal's non-causal associations) resonates with the science that makes the absolute violence of the atomic bomb possible, as well as with the idea of uncertainty in the social world. Taking Edkins' argument to our concern here – the deployment of algorithms in everyday securitization – we can point to a coalescence between indeterminacy in the physical sciences, the emergence of virtual and 'network' warfare, and the rise of inference and suspicion in the security decision. What *is novel* in the contemporary moves to algorithmic war, then, is the specific form that the aligning of science, commerce, military and the state is taking.

In the emerging geography of algorithmic war, the relationships between science, expertise and decision are radically rearticulated so that distinctions between "science" and "non-science", "expert" and "inexpert" knowledge become more malleable. It is not strictly the case, then, as Richard Ericson and Aaron Doyle have it, that where "scientific data on risk is absent" there is a turn to "non-scientific forms of knowledge that are intuitive, emotional, aesthetic, moral, and speculative" (2004: 138). Instead, on the one hand, scientific data begins to incorporate the emotional, affective and speculative domains while, on the other, knowledges considered to be "non-scientific" are authorized as science. Data-led algorithms that model and track the movement of bodies or objects

through space now coalesce with intuitive, speculative and inferential knowledges that imagine future scenarios.

Consider, by way of example, the multiple interacting forms of algorithmic knowledge that are emerging in the transitory spaces of the subway. Surveillance cameras, equipped with facial and gait recognition technologies, track 'atypical' movements such as repeated traversals of a platform (Hale 2005); 'smart' travel payment cards store journey data and identify anomalies; and poster displays urge the public "if you suspect it, report it".[2] The calculations of the algorithm appear to translate the observation of uncertain and contingent human life into something with the credibility of scientific judgement. The UK's Metropolitan Police public vigilance campaigns, for example, use algorithms on the screens of 'terror hotline' call centres, ascribing a level of scientific and technical certitude to the reported suspicions of the 'out of the ordinary'.[3] The specific deployment of scientific knowledge, then, incorporates the affective domain, rendering fears and anxieties a means of anticipating the future. "The precautionary principle", writes François Ewald, "presupposes a new relationship with science and with knowledge", one which "invites one to anticipate what one does not yet know, to take into account doubtful hypotheses and simple suspicions" (2002: 288). Algorithmic security technologies allow the embracing of the precautionary principle in just this way, inviting anticipatory actions and making scientific and certain what would otherwise be mere uncertain doubts or suspicions.

If algorithmic techniques are concerned with anticipating an uncertain future, then the logic of algorithmic war is one of identifying norm and multiple deviations from the norm. To be clear, this is not the norm that is familiar to studies of disciplinary society. As Foucault explains, "disciplinary normalization posits a model and tries to get people, movements, and actions to conform to this model [the norm]" (2007: 57). In the security apparatus, by contrast, we find "exactly the opposite of the disciplines", where we have "a plotting of different curves of normality… the interplay of differential normalities" (63). Understood in this way, the algorithm becomes a very specific modality of the "imaginative geography" of the war on terror. It plays it part in making possible the

interplay of differential normalities – not forever settling out normal and abnormal, permitted and prohibited, but allowing degrees of normality.

Citing international relations scholar Michael Shapiro, Derek Gregory argues that "geography is inextricably linked to the architecture of enmity", to the overlapping practices through which "collectivities locate themselves in the world and thus how they practice the meanings of Self and Other that provide the conditions of possibility for regarding others as threats or antagonists" (2004: 20). Yet, Gregory's "spiraling networks" do not fully push the limits of Shapiro's architecture because they return the geopolitics of violence to the disciplinary norms of battlefield spaces, obscuring the subtle differential violences of the "surveillance network" of the "end-of-violence organization" that Shapiro later depicts (2004: 121). In the name of homeland security (the end of violence), algorithmic war reinscribes the imaginative geography of the deviant, atypical, abnormal 'other' *inside* the spaces of daily life. The figure of enmity to be feared and intercepted need not only dwell in a represented *outside* in the geographies of Iraq or Afghanistan, for the outside can be inside – in the body of the migrant worker (differentially normal in the space of the economy and abnormal in the spaces of immigration), the young Muslim student (permitted to study but observed in the college's Islamic society), the refugee (afforded the hospitality of the state but biometrically identified and risk rated), the British Asian traveler (granted visa waiver but ascribed an automated risk score).

Thus, the emergent geography of a twisted and conjoined figure of inside and outside, where "one does not know on which face of the strip one is located" (Bigo 2001: 115). For Didier Bigo, this is a spatiality of the policing of multiple and variant lines between self and other, an "everyday securitization from the enemy within" (2001: 112). Here the architecture of enmity becomes the means of securitization itself, such that the distinction between 'real' war (with accompanying visceral violence and bloodshed) and the war by other means (legitimated by securing against future violence) becomes permeable. The network warfare depicted in accounts of a "military-industrial-media-entertainment (MIME) complex", where "information is no longer a subsidiary of war", extends the

stealthy war-like practices "more widely and deeply into our everyday lives (Der Derian 2002; see also Dillon and Reid 2007). Consider, for example, the Oracle Corporation's software, already ubiquitous in our lives, providing IT platforms for payroll, pensions, health care, the bibliographic searches used in academic research, and so on. Their algorithmic security systems - Non-Obvious Relationship Awareness (NORA) software – developed for the entertainment industry and used in the Las Vegas casinos – are now deployed by the US Justice and federal intelligence agencies for counter-terror. According to Oracle consultants, NORA enables clients to identify "obscure relationships between customers, employees, vendors, and other internal and external data sources". NORA searches for behaviour patterns or personal associations that hint at terrorist activity, turning data into actionable intelligence" (IDC 2004: 11).

The association rules of the algorithm claim precisely to identify associations, to connect together *here* and *there*, to link *that* location of suspicion and *this* embodied risk, to suture together the forces of war in one place and the possibility of threat in the spaces of everyday life. In essence, as it traverses the spheres of commerce and consumption, transportation, military strategy and state surveillance, the algorithm simultaneously conceals the architecture of enmity through which it functions. Giving the appearance of an advanced security decision based on the technical and scientific computation of norms and deviations from norm, beneath its skin the algorithm contains all of the categories, codes and measures that we see in other violent geographies – the racial profiles embedded within biometric facial measures, the ethnic or religious practices flagged as anomalous in air passenger data, the identification of risk by algorithmic screening of name or address. These are the more subtle violences of science and state that are not measured by a linear experience of harm, but instead attach themselves to daily prosaic practices, limiting the possibilities for life, of life itself (Das and Kleinman 2000).

Locatability/Security: Sensors at the Border and in the Supply Chain

In August 2004, the US Department for Homeland Security (DHS) announced the testing of a new tracking technology at five US land border ports of entry. The trial – conducted by consultants *Accenture* and *Deloitte* in collaboration with *Philips Semiconductors* – embedded radio frequency identification (RFID) tags into paper I-94 customs and border protection forms.[4] The RFID tags contain a 'passive' chip and antenna, capable of transmitting a unique numeric identifier to a remote reader. By October 2006, though rejected for US passports, the same RFID technology became a US entry requirement for visa waiver programme passports. Later the same year, the UK's Transport for London announced that its RFID-enabled Oyster travel payment card was to integrate with a Visa credit card, allowing the tracking and tracing of all small transactions, actions and movements on the London Underground system.

How might we understand what is at work here? A virtually invisible technology, concealed within a paper document or 'smart' card, is deployed with the precise purpose of rendering a person visible, identifiable and locatable. As architect Dana Cuff has noted, "there is an irony here", it is "invisible, miniaturized sensors that are making formerly inaccessible realms visible" (2003: 45). In part, of course, the apparent invisibility of the techniques for making visible is assured because of their already existing ubiquity in everyday commercial transactions. As the Vice President of *Philips Semiconductors* had testified to the US Congress Committee on Energy and Commerce in 2004, "consumers are already likely to encounter RF-enabled personal identification devices in their daily lives, such as secure access cards for building entry, speedy gasoline purchasing such as the *Exxon Speedpass*, vehicle anti-theft systems, and in transportation systems all over the world" (US House of Representatives 2004: 3). What is taking place, then, is the redeployment of sensor technologies used in the commercial tracking of mobile things, objects, animals and vehicles into the domain of the tracking of mobile people.

As a technology of location, tracking is central to the processes and practices of militarization. As performance artist and social theorist Jordan Crandall has argued, "militarization and movement intersect through the activity of tracking" (2005: 19). The

domains of geopolitics and geoeconomics cross over here (see Cowen and Smith, this issue) as the governing of the global economy draws into common assemblage with a state that is concerned to make visible the minutiae of daily life, to seek security in the transactions, journeys and movements that are the norm and those that are suspicious. Put simply, algorithmic war requires a *target* for its calculations, preferably a moving target. The practice of tracking, then, seeks to "detect, process and strategically codify a moving phenomenon in a competitive theatre", whether this space is a "battlefield, the social arena, or the marketplace" (Crandall 2006: 4). In this sense, tracking technologies enable the identification and location of moving targets. In the war on terror, the specific form has become what Samuel Weber calls a "target of opportunity", a competitive "seizing" of "targets that were not foreseen or planned" (2005: 4). The targets of opportunity in the war on terror, then, involve the depiction of mobile enemies:

> However different the war on terror was going to be from traditional wars, with their relatively well-defined enemies, it would still involve one of the basic mechanisms of traditional hunting and combat, in however modified and modernized a form: namely "targeting". The enemy would have to be *identified* and *localized*, *named* and *depicted*, in order to be made into an accessible target… None of this was, per se, entirely new. What *was*, however, was the mobility, indeterminate structure, and unpredictability of the spatio-temporal *medium* in which such targets had to be sited… In theatres of conflict that had become highly mobile and changeable, "targets" and "opportunity" were linked as never before.
>
> (Weber 2005: 3-4, *emphasis in original*).

Samuel Weber's key point of discussion is the theatre of war, though his argument sheds significant light on the algorithmic wars on terror that I depict here. The *identification*, *localization*, *naming* and *depiction* of mobile targets is, in this war by other means, conducted in and through daily life, in advance of any possible future strike or intervention. The targeting of mobile bodies, things, objects or monies is becoming a matter of locating – positioning in the sights, if you like – so that the opportunities of a mobile global economy might be seized, while the capability to take out the target

remains. “Freedom is nothing but the correlative of the deployment of apparatuses of security”, states Foucault, “the very possibility of movement, change of place, and processes of circulation of both people and things” (2007: 49). For this reason, the geography of algorithmic war is a spatiality of *locatability in movement*, with origins in the interplay between military logistics and the commercial logistics of tracking objects through a supply chain. As consultants *Accenture*, *Deloitte*, *IBM* and *PricewaterhouseCoopers* lead the drive for multiple networked public and private applications of technologies of location such as RFID, the commercial “targets of opportunity” that allowed the production of goods to become dispersed and diffuse are clearing space for more diffuse modes of sovereign power. The technologies that have made possible a global supply chain of export processing zones and offshore sites, are simultaneously being embedded into border crossing cards, visas, passports and immigrant ID cards that include mobile people within governable space by means of their targeted exclusion.

How has locatability emerged as a key means of tracking mobile targets? The emergence of knowledges of location, what Nigel Thrift has called “our conventions of address”, follows a tacit and often unacknowledged sense that we somehow know “what will show up where and what will show up next” (2004: 176). In other words, a system of address has been central to our ability to spatially and temporally locate events, objects, people and so on. The history of addressability displays a significant playing back and forth of military logistical knowledges and commercial supply and transportation knowledges. Thus, for example, the origins of 1940s bar code technologies lie in the communication techniques of Morse code. Historical records of early bar code techniques describe a graduate student, Joseph Woodland, marking the dots and dashes of Morse code into the sand on a beach as he thought through a research problem of how to identify a product at a check-out (Shepherd 2004: 13). Extending the dots and dashes to two-dimensional wide and narrow lines in the sand, Woodland later successfully patented the first binary barcode system.

As computing technologies began to enable the electronic reading and recognition of patterns, new relationships between the identifier (postal code, ZIP, barcode, personal identifiers such as date of birth) and the identified (people, places, parcels, vehicles..) become possible. Consider, for example, IBM's 'punch cards' of the 1950s, patterns of punched holes in a card to be fed into the pattern recognition programmes of IBM machines.[5] The "patterns of data on the IBM cards", writes architect Reinhold Martin, "made visible what was invisible" (2003: 158). The machine's ability to 'read' the cards extended beyond the mere processing of data and into the almost magical realm of animating a life unseen. In a 1955 publicity brochure, IBM reminded the American public of how their lives were locatable in the traces of actions and transactions left in the card and 'read' by the machine:

> IBM first came into your life when your birth was recorded on a punched card. From then on many such cards have been compiled, giving a lifetime of history of your important decisions and actions. If you went to school, entered a hospital, bought a home, paid income tax, got married or purchased an automobile, the chances are that permanent records were made of these and other personal stories.
>
> (Cited in Martin 2003: 159).

What we begin to see with the intersection of systems of address with systems of recognition, or the marrying of addressability and readability, if you like, is a computer-enabled system of *locatability*. While even rudimentary systems of address involve recognizing identifying markings, whether these are numbers, features of the natural landscape, or codes, the computer reading of markings and the recognition of patterns makes possible novel forms of location. Here, the emphasis is on a more mobile and agile mode of address that does not 'stop at the door' of delivery, but instead dwells inside, making visible, readable and locatable the traces of daily life. With the rise of what Jerry Kang and Dana Cuff call "computer addressability", the fixed location of the address is loosened via "unique identification codes" (2005: 94). Because the codes dwell inside a body or object in the physical environment, they do, at least in theory, make it locatable in movement.

In this shift from addressability to locatability, the ability to track and trace mobility is achieved by animating the physical environment so that it is able to "respond directly to what it sees" (Kang and Cuff 2005: 94). Thus, the 'reader' of traces, markings or transactions, established via the early technologies of punch cards and barcodes, becomes ever more important to the system of location as "addresses move with human and non-human actants" (Thrift 2004: 183). Rather as IBMs early computers inferred people's life histories from the patterns punched into the cards, and from the intervals between them, contemporary readers of location, as a group of researchers at Intel have put it: "infer people's actions from their effect on the environment, especially on the objects with which they interact" (Smith et al. 2005: 39). The embedding of RFID tags into objects, as Smith and his colleagues have shown at Intel, can be understood as one means to achieve a novel and mobile form of targeting.

The origins of contemporary RFID technology, perhaps unsurprisingly, also find some roots in military communications and logistics, with the earliest writings on the problem to be found in research by radio engineers seeking more efficient readability of signals (Stockman 1948). It should be clear, then, that we cannot say that contemporary security applications of RFID are simply drawing on commercial knowledges of location. The 1940s research was, in many ways, the precedent for contemporary RFID technologies that deploy miniature tags, emitting a radio signal with a unique numeric identifier that can be received by a reader up to 25 feet away (Borriello 2005). Composed of a silicon chip and coiled antenna, usually sandwiched inside a plastic tag, so called 'passive' RFIDs use the power supply from the reader to send their signal and are, therefore, smaller and require closer proximity to the reader than 'active' tags that carry their own power supply. For example, a passive RFID application such as a supermarket loyalty card that is read at the till is, in effect, inert until it is in range of the reader that activates it. Once in range of the reader, the RFID's numeric identifier allows the reader to locate the tag and to associate data on past readings of transactions. For a supermarket shopper's 'loyalty card' this might include patterns of past purchases, coupons or vouchers for savings and such like. For a US-Mexico border crossing card holder, the passive tag

signals an identifier that can be mapped across past patterns of travel, criminal convictions or terrorist watch lists. In this way, the RFID identifies the target for algorithmic calculation, at the border, at the supermarket check-out, at the entrance to the sports stadium, in the subway ticket hall. "Through RFID tags", as Jerry Kang and Dana Cuff have it, address is specified "to a fine level of granularity, much finer than a zip code", so that we "will likely authenticate our identity to multiple queries of 'who are you' made by the enacted environment" (2005: 106).

What are the implications of mobile forms of locatability for algorithmic war and, in particular, for the exercise of sovereign power? As RFID stands on the brink of replacing bar code and paper-based markers of location (I 94 forms, passports, train tickets, paper money at toll booths, tickets for sports events),[6] how does the war on terror become enmeshed with the geographies of everyday life? To be clear here, the seizing of targets of opportunity by commercial players can in no sense be interpreted as transcending the nation-state or outsourcing state security decisions to the market. Rather, a logic of outsourcing and targeting that exceeds any specific public or private domain – that is, as Samuel Weber suggests, a "militarization of thinking" – works to sustain the "hyphen" in the imagination of nation-state differently (Sparke 2005: 48). It does so, I will argue here, via a spatial and temporal *deferral of security decision* that follows the dispersed geography of the commercial supply chain.

The state's ability to track and trace people or objects in movement, across or beyond its borders, is increasingly bound up with commercial techniques for tracking and tracing objects through the supply chain. The paradox of security and mobility – the problematic of the moving target – is given the appearance of being fixed by technologies of locatability. As David Campbell writes, "were it possible to bring about the absence of movement", that would represent "pure security", yet it would be at that moment that "the state would wither away" (1992: 12). The question is not one of how to arrest mobility, then, but how to govern mobility in such a way as to allow circulation and to sustain the impression of securability. Put simply, to secure the sovereign power of the

state in a global economy of mobile things and people precisely by means of targeting bodies in movement.

The contemporary decentred state shares much of its spatial character with the diffuse and dispersed capillaries of global capital. If William Connolly (2005: 148) is correct and sovereignty is "migrating to a layered global assemblage", then one aspect of this layering is the profusion of ambiguous locations of many kinds, where the distinctions between legality and illegality, work and violence, onshore and offshore are increasingly blurred. Just as the dispersal of a global supply chain into offshore sites and export processing zones permits the deferral of many kinds of commercial decision – at least in terms of Jacques Derrida's sense of decision as responsibility (1995: 25) – so the diffusion of state authority into ambiguous locations of many kinds appears to institute the deferral of decision on behalf of the state. In the marketplace that is the test laboratory for RFID applications, for example, the tagging at item level by *Wal-Mart*, *M&S* and *Gillette* has allowed these commercial players to seek efficient locations in distant places, and yet to sustain the ability to control with precision (Eckfeldt 2005). The very idea of an animated supply chain, making its own algorithmic calculations and judgements – from "smart refrigerators" to smart supermarket shelving and tracked shipments (Günther and Spiekerman 2005) – incorporates the bodies and objects of production and consumption, from the growers, pickers and producers of raw materials, through manufacturing, supply and retail workers.

In the most vulnerable offshore spaces of the global economy, where commercial firms seek only the most fleeting of finger holds in a specific territorial space, we begin to see how the commercial targeting of things and objects plays into and through the targeting of people. Thailand's export processing zones – or 'free zones' – for example, have become "e-free-zones", using RFID to track the movement of imported materials, deliveries, exported goods, and, significantly, the bodies of workers, as they traverse the boundaries of the zone. The fortified security fences associated with export processing zones, then, are augmented by equally carceral, but less obviously visible, lines that track and trace the movements of workers via "contactless" smart cards, and the mobility of

objects via RF enabled smart labels. Similarly, the extension of RFID into border crossing cards and immigration documents allows the feigned impression of an open world, while it institutes new lines and boundaries. There is a growing resonance, then, between apparently geo-economic systems of locatability (of course always also political) that target the bodies of workers and the movement of the objects with which they interact, and the algorithmic security practices of the state:

> It plays out in new systems of production that aim to narrow the intervals between conception, manufacturing, distribution and consumption – shrinking the delays between detecting an audience pattern and formatting a new enticement that can address it. It plays out in pre-emptive policing and warfare systems that aim to close the gap between sensing and shooting.
>
> (Crandall 2006: 13).

As Jordan Crandall depicts the geographies of tracking and targeting, they play in and out of the plural spaces of our world. As the commercial tracking technologies enter the sphere of security – RFID passports, 'smart' national ID cards, RF-enabled immigration and visa documents, the tagging of detained asylum seekers, employee 'contactless' buildings access cards – they defer security decisions into algorithmic calculation. The participation of RFID in violent geographies is thus often obscured. When global consultants Accenture made their successful bid for the USVISIT 'Smart Borders' contract, for example, they simulated the ability of RFID to target from a distance:

> Using a nearby facility belonging to *Raytheon*, a subcontractor on its team, the Accenture team constructed a mock border point kiosk at which the government team had an RFID tag attached to their passports. They also constructed a mock land border crossing where a scanner read the RFID passport tags of the government officials inside the car. Even though the car became momentarily airborne after hitting a speed bump – the scanner read the digital information contained on the RFID chips of all four government officials in the vehicle, displaying their pictures on an electronic billboard as they passed by.

(Accenture 2005: 242, *emphasis added*).

Accenture's business partner *Raytheon*, the world's largest manufacturer of so-called 'smart weapons', produces the cluster bombs widely reported to be responsible for the violent deaths of civilians in Iraq and Afghanistan. Here we see the targeting of markets and neighbourhoods by military hardware segueing into the targeting of people at border crossings and in the spaces of the airport. Indeed, it is *Raytheon* that, in November 2007, was awarded the £650 million UK e-borders contract as the leading contractor of the *Trusted Borders* consortium, with *Accenture* the IT systems subcontractor. Where RFID appears to render movement around the subways, highways and superstores of the global economy as a smooth and seamless experience, it does so by aligning the security practices of the state with the mobilities of the consumer. In this sense, our everyday geographies do spiral into and across the daily violences of the algorithmic targeting of 'others' and the visceral military violence of bombing campaigns.

It is important to recognise at this point that we can only gain a limited understanding of the technologies of algorithmic war by seeing them as explainable by the post 9/11 deepening of political economies of surveillance (Lyon 2003). The capacity of RFID to make us locatable is actually acutely ambivalent: we feel its potential to watch and to incarcerate just as we simultaneously feel it fulfil some of our desires and pleasures. As Matt Sparke has illustrated in his study of the biometric proximity cards used in the US-Canadian border NEXUS programme, the appeal is made to "the fast lane, where you want to be" (2006: 167). Similarly, RFID is offered as a means of expediting mobility in the UK's Heathrow airport "MiSense" programme, promising to "simplify your journey through the airport while maintaining security".[7] The *MiSense* programme, by incorporating smart sensors into the possession of the subject – 'my sense' – invites an almost playful encounter with RFID sensors. This stitching together of playful leisurely RFID encounters with security practice asks the subject to voluntarily offer themselves up to tracking technologies in return for expedited movement. In some of the most playful forms of RFID use in the leisure industry – subcutaneous chips inserted into the arms of customers at a Glasgow nightclub so that they may pay for their drinks without

the hindrance of cash or cards; RFID golf balls that communicate their location to a remote reader – we can see security dreams fulfilled. Night club patrons secure their pre-cleared identity and financial details beneath their skin, and golfers seek out a means of securely locating distant objects. Where RFID "pleasures and anxieties cohabit", the targeted line of sight sorts and segregates finite degrees of visibility so that, for some, "the edges are smoothed" as they "blend seamlessly into the crowd" (Crandall 2006: 12). For others, of course, the line of sight targets for heightened exposure to visibility – to stop and search, to continually verify identity, to have movement in public space checked and intercepted.

Conclusions: Securability and Algorithmic War

> You won't get by the booth… You look too young to be driving out of state"… But there is nobody in the booth built to hold a toll-taker. Nobody. A green light flashes E-Z PASS PAID and Ahmad and the white truck are admitted to the tunnel.
>
> (Updike 2006: 298).

In a final scene of John Updike's novel *Terrorist*, the protagonist Ahmad drives his truck bomb to the entrance of the Manhattan-bound Lincoln tunnel. His passenger and reluctant mentor, Jack Levy, urges him that the security guard will detain him on the grounds that he looks too young to have a state license permitting him to drive out of state. At the boundary line of the city, Levy feels sure, their fatal journey will be halted, their movement intercepted. What Levy does not anticipate is the RFID transponder on the windshield of the truck, sending a signal to the barrier reader, algorithmically calculating – is the truck licensed?; is the toll pre-paid?; has the vehicle been reported stolen? The calculation is made, a green light flashes and the truck enters the tunnel.

In Updike's novel, the practices of homeland securitization are revealed in all their contingency and unpredictability (asked by his wife what the Homeland Security

department's elevation of threat from yellow to orange means, Levy replies "It means they want us to feel they have a handle on this thing, but they don't"). The algorithmic technologies, so readily established at the forefront of the securitization of borders and boundaries of many kinds, are revealed in Updike's novel to be intrinsic to the feigning of securability. The point here is that we know not, in any meaningful sense, what algorithmic war will do beyond giving the impression that things/people/commodities can be secured against an imagined enemy. It could have been the case – had the association rules shown the white truck to be on a watch list database, or the E-Z Pass to be expired, or had a previous transaction flagged a risk – that the algorithm signalled a red light and the movement of the truck would have been intercepted. Yet, these are the contingencies of the relationship of the algorithmic calculation to the actual everyday geographies they seek to model and simulate. These are the unknowns, the indeterminacies of algorithmic war.

The question, then, is how to open up these contingencies and ambiguities in order to politicize what would otherwise be a highly technologized set of moves. "Uncertainty and unpredictability can be unsettling", writes Jenny Edkins, "in the rational west, we tend to seek certainty and security above all. We don't like not knowing. So we pretend that we do" (2003a: 12). The algorithmic war I have described here – with its dividing geographies of us/them, safe/risky – is precisely one means by which we "pretend that we do". Algorithmic logics appear to make it possible to translate probable associations between people and objects into actionable security decisions, or to incorporate the uncertain future into the present. The practices of this war by other means, then, are themselves productive of quite specific pre-emptive forms of war and violence. Though the everyday geographies of this 'other' war on terror are partially *militarizing*, in the sense of drawing military practice more closely into proximity with everyday life, they are more meaningfully drawing on a militarization of thinking that is co-present in corporate calls for risk targets and the riding out of uncertainty, in state drives to target, track and trace people and objects, and in the suspicions and prejudices of an enlisted vigilant public.

References

Accenture (2005) *Values, Driven, Leadership: The History of Accenture*, Chantilly VA: History Factory.

Accenture Digital Forum (2004) 'US DHS to develop and implement US VISIT program', available at www.digitalforum.accenture.com, last accessed February 2007.

Agrawal, Rakesh, Tomasz Imielinski and Arun Swami (1993) 'Mining Association Rules Between Sets of Items in Large Databases' *SIGMOD Proceedings* pp.914-925.

Aitken, Rob (2006) 'Capital at its Fringes', *New Political Economy* 11:4

Amoore, Louise (2007) 'Vigilant Visualities: The Watchful Politics of the War on Terror, *Security Dialogue* 38: 2.

Amoore, Louise (2006) 'Biometric Borders: Governing Mobilities in the War on Terror', *Political Geography* 25: 3, pp.336-351.

Amoore, Louise and Marieke de Goede (2005) 'Governance, Risk and Dataveillance in the War on Terror', *Crime, Law and Social Change* 43, pp.149-173.

Baker, Tom (2002) 'Liability and Insurance after September 11: Embracing Risk Meets the Precautionary Principle', *University of Connecticut School of Law Working Papers Series*. 4

Bigo, Didier (2001) 'The Möbius Ribbon of Internal and External Security(ies)', in M. Albert, D.Jacobson and Y.Lapid (eds) *Identities, Borders, Orders: Rethinking International Relations Theory*, Minneapolis: University of Minnesota press.

BMSA (2004) *The Mathematical Sciences' Role in the War on Terror*, National Academies Press.

Borriello, G. (2005) 'RFID: Tagging the World', *Communications of the ACM* 48, pp.34-37.

Campbell, David (1992) *Writing Security: US Foreign Policy and the Politics of Identity*, Manchester: Manchester University Press.

Chalfin, Brenda (2004) 'Border Scans: Sovereignty, Surveillance and the Customs Service in Ghana', *Identities: Global Studies in Culture and Power* 11, pp.397-416.

Chertoff, Michael (2006) 'A Tool we Need to Stop the Next Airliner Plot', *Washington Post,* August 29: A15.
Computing (2004) 'Government Confirms IBM's Semaphore Win', November 3 2004.
Crandall, Jordan (2006) 'Precision+Guided+Seeing', C.theory.net/articles.aspx?id=502.
Crandall, Jordan (2005) 'Envisioning the Homefront: Militarization, Tracking and Security Culture, *Journal of Visual Culture* 4: 1, pp.5-15.
Connolly, William (2005) *Pluralism*, Durham and London: Duke University Press.
Cuff, Dana (2003) 'Immanent Domain: Pervasive Computing and the Public Realm', Journal of Architectural Education, pp.43-49.
Das, Veena and Arthur Kleinman (2000) 'Introduction', in Veena Das, Arthur Kleinman, Mamphala Ramphele and Pamela Reynolds (eds) *Violence and Subjectivity*, Berkeley: University of California Press.
De Goede, Marieke (2003) 'Hawala Discourses and the War on Terrorist Finance,' *Environment and Planning D: Society and Space* 21 (5): 513-532.
Department of Homeland Security (2006) 'Survey of DHS Data Mining Activities', Washington DC: Office of the Inspector General.
Department of Homeland Security (2003) 'US VISIT Begins Testing RFID Technology to Improve Border Security and Travel', press release August 8, available at www.dhs.gov/xnews/releases/press_release_0713-shtm last accessed November 2006.
Der Derian, James (2002) 'The War of Networks', *Theory & Event* 5: 4.
Derrida, Jacques (1999) *The Gift of Death*, Chicago: University of Chicago Press.
Dillon, Michael and Julian Reid (2007) *The Liberal Way of War*, London: Routedge.
Eckfeldt, Bruce (2005) 'What Does RFID Do for the Consumer?', *Communications of the ACM* 48: 9, pp.77-79.
Edkins, Jenny (2003a) *Trauma and the Memory of Politics*, Cambridge: Cambridge University Press.
Edkins, Jenny (2003b) 'Security, Cosmology, Copenhagen', *Contemporary Politics* 9: 4, pp.361-370.
Edwards, Paul N. (1996) *The Closed World: Computers and the Politics of Discourse in Cold War America*, MIT Press.

Ericson, Richard and Aaron Doyle (2004) 'Catastrophe Risk, Insurance and Terrorism', *Economy and Society* 33: 2, pp.135-173.
Foucault, Michel (2003[1976]) *Society Must be Defended: Lectures at the Còllege de France*, New York: Picador.
Foucault, Michel (2007[1977]) *Security, Territory, Population: Lectures at the Còllege de France*, Basingstoke:Macmillan.
Graham, Stephen (ed.) (2004) *Cities, War and Terrorism: Towards an Urban Geopolitics*, Oxford: Blackwell.
Gregory, Derek and Alan Pred (eds) (2007) *Violent Geographies: Fear, Terror and Political Violence*, New York: Routledge.
Gregory, Derek (2004) *The Colonial Present*, Oxford: Blackwell.
Guild, Elspeth and Evelien Brouwer (2006) 'The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US', *CEPS Policy Brief* 109, www.libertysecurity.org/IMG/pdf/1363.pdf
Ewald, François (2002) 'The Return of Descartes's Malicious Demon: An Outline of a Philosophy of Precaution', in Tom Baker and Jonathan Simon (eds) *Embracing Risk: The Changing Culture of Insurance and Responsibility*, Chicago: University of Chicago Press.
Hacking, Ian (1990) The Taming of Chance
Hale, Benjamin (2005) 'Identity Crisis: Facial Recognition Technology and the Freedom of the Will', *Ethics, Place and Environment* 8: 2, pp.141-158.
IDC (2004) 'Identity Management's Role in an Application-Centric Security Model', White Paper, Framingham MA: IDC.
Intelligent Enterprise (2002) 'For Want of a Nail', 5:7, p.8.
Kang, Jerry and Dana Cuff (2005) 'Pervasive Computing: Embedding the Public Sphere', Public Law Research Paper Series no.04-23, Los Angeles: University of California.
Katz, Cindi (2007) 'Banal Terrorism', in Gregory, Derek and Alan Pred (eds) (2007) *Violent Geographies: Fear, Terror and Political Violence*, New York: Routledge.
Light, Jennifer (2003) *From Warfare to Welfare*, Baltimore MD: Johns Hopkins University Press.

Martin, Reinhold (2003) *The Organizational Complex: Architecture, Media and Corporate Space*, MIT Press.
New York Times (2006) 'Private Sector Entices Anti-Terror Officials', June 18 pp.6-18.
Quinlan, J.R. (1986) 'Induction of Decision Trees', *Machine Learning* 1, pp.81-106.
Science News (2006) 'Beyond Bar Codes: Tuning Up Plastic Radio Labels', *Science News* 169: 6.
Shapiro, Michael (1997) *Violent Cartographies: Mapping Cultures of War*, Minneapolis: University of Minnesota Press.
Shapiro, Michael (2004) '"The Nation-State and Violence": Wim Wenders contra Imperial Sovereignty', in Jenny Edkins, Veronique Pin-Fat and Michael Shapiro (eds) *Sovereign Lives: Power in Global Politics*, New York; Routledge.
Smith J.R. et al. (2005) 'RFID-based techniques for human-activity detection', *Communications of the ACM*, 48: 9, pp.39-44.
Sparke, Matthew (2005) *In the Space of Theory: Postfoundational Geographies of the Nation-State*, Minneapolis: University of Minnesota Press.
Sparke, Matthew (2006) 'A neoliberal nexus: economy, security and the biopolitics of citizenship on the border', *Political Geography* 25(2): 151-180.
Stockman, H. (1948) 'Communicating by Means of Reflected Power', *Proceedings of the Institute of Radio Engineers*, October, pp.1196-1204.
Thrift, Nigel (2004) 'Remembering the Technological Unconscious by Foregrounding Knowledges of Position', Environment and Planning D: Society and Space 22, 175-190.
US Department of Justice (2002) 'Hearing on the financial war on terrorism and the administration's implementation of the anti-money-laundering provisions of the USA PATRIOT Act', Washington DC: US Senate Committee on Banking, Housing and Urban Affairs.
US Joint Inquiry (2003) 'Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001', Washington DC: House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI).
Weber, Samuel (2005) *Targets of Opportunity: On the Militarization of Thinking*, New York: Fordham University Press.

Acknowledgements
This article was first presented at the 'Militarization, Society and Space' symposium, Institute of Geography, University of Edinburgh, 23 November 2006. Profound thanks are due to Andrea Nightingale and Jane Jacobs for their inspirational event and for their comments on the paper that emerged as a result. Deb Cowen and two anonymous reviewers have also made important interventions that I hope I have done some degree of justice to. Funding for the research of which this paper is part is provided by ESRC, 'Data Wars: New Spaces of Governing in the European War on Terror', award number RES 062230594, with Marieke deGoede (Amsterdam).

NOTES

[1] Among the 34 items of passenger data required under the EU-US passenger name record (PNR) or Advance passenger information system (APIS) agreement, legally challenged by the European Court of Justice in 2006, are credit card details, criminal records and in-flight meal choices. The data is extradited to the US within 15 minutes of flight departures from Europe (Guild and Brouwer 2006).

[2] In 2005, London's Metropolitan Police launched a public vigilance campaign, 'If you suspect it, report it', that has now been extended across the UK. The campaign urges people to report "suspicions about somebody's behaviour" to an anti-terrorist hotline (Metropolitan Police 2005).

[3] The call centre operator will ask the caller questions about the nature of the suspicion, generating a risk profile from the associations between different items of information – how many trains have passed the platform?; what type of clothing?; carrying a bag?; alone or accompanied? (insights from confidential interview conducted London, November 2006).

[4] The green paper I-94 documents are familiar to visa waiver citizens as the declarations completed on airline flights to the United States.

[5] IBM's generation of punch-card computers used technology derived from Herman Hollerith's patterned cards developed for the US census of 1890, itself having roots in pattern cards used in weaving (Hacking 1990: 53). The IBM Hollerith technologies and techniques were used in the Nazi death camps to identify individuals and to track the 'transports'. After the War, Hollerith machines were also deployed by the Red Cross to trace survivors.

[6] At an electronics conference in San Francisco in February 2006, researchers from Philips' laboratories in the Netherlands announced their new RFID chips with plastic in place of silicon semi-conductors. According to Science News, the replacement of silicon "brings closer the prospect of RFID tags becoming as common as bar codes, or perhaps even more so as plastic tags make novel electronic tracking and transactions possible, from computer monitoring of what is in the refrigerator to mail routing by means of smart address labels" (2006: 1).

[7] Full text of the miSense programme is available at www.misense.org, last accessed December 2006.