The international ‘data war’ that is fought in the name of counter-terror is concerned with mobilising the uncertain future to intervene ‘before the terrorist has been radicalised’. Within this project, the digital footprint has become increasingly significant as a security resource. At the international border, particularly, the traces of data that cannot help but be left behind by everyday consumption and travel activity are mobilised within ‘smart’ targeting programmes to act against threat ahead of time. Subject to analytics, rules-based targeting and risk-scoring, this data is believed to offer a fuller picture of the mobile subject than conventional identification information. This paper places the data footprint alongside the history of the conventional criminal ‘print’ within forensic science to examine the future-oriented modes of governing that are emerging within smart border programmes such as the UK’s e-borders. The digital print has less in common with the criminal print as objective evidence of past events and more in common with early efforts in anthropometry and biometrics to diagnose a subject’s proclivity ahead of time. In the context of contemporary border security, this is unleashing uneven and occluded governmental effects.

KEYWORDS: digital footprint; border security; e-borders; PNR; preemption

We must move from chasing threats to anticipating them well ahead of time, hypothesising threat blueprints or ‘threatprints’ that can be broken down into their component parts. Our objective must be to anticipate needles before terrorists or criminals have even thought to place them within the haystack. In fact, even before the terrorist or criminal has been radicalised or recruited in the first place. (Detica 2008a, p. 2)

Introduction

In 2008, IT security consultancy Detica outlined its approach to data analytics in homeland security. In a paper entitled ‘The Information Revolution and its Impact on Homeland Security’, Detica describe a contemporary ‘data tsunami’ that constitutes a threat, but which also holds a ‘silver lining’:

Every threat of any significance anywhere in the world has a digital footprint – a trail of ones and zeros – that terrorists and criminals leave behind on the Internet and in other electronic databases . . . If we can discover these digital footprints then the most serious threats to our security and way of life can be defeated. (Detica 2008a, p. 4)

What is required from contemporary security data analytics, argues Detica, is an approach that can deal with ever-increasing amounts of data to provide ‘effective threat intelligence capability’ able to uncover ‘the digital footprints laid down by those who threaten the
security of the state . . .' The ‘digital footprint’ that is ‘laid down’ in databases and digital transactions has come to occupy a prominent position in the fight against terrorist and criminal activity in the war on terror. When ‘terrorists can appear unremarkable in the real world’ and when criminals’ ‘real world footprint’ is decreasing (Detica 2008a, p. 4, 2008b), the digital footprint appears to constitute an objective, efficient way of identifying threatening activity from the traces it leaves behind.

At the border, particularly, the digital footprint that is believed to betray terrorist and criminal activity has become increasingly important for security. Border targeting systems such as the UK e-borders programme and the US Automated Targeting System gather and analyse a range of passenger data as a means of combating security threats. Detica, for instance, has been responsible for developing intelligence and analytics solutions for the UK e-Borders programme, subjecting categories of passenger data to algorithmic and associative analysis to uncover ‘actionable intelligence’. Increasingly, this data is not simply personal information submitted for visa applications, or data encoded in passports more conventionally associated with identification. Rather, data that is generated by commercial transactions (notably the Passenger Name Record) is becoming an important way of identifying high-risk activity. ‘Unknown’ terrorists and criminals may not be flagged up by watchlist checks, but the screening of passenger data against indicators of risk (unusual itineraries, associations with known suspects, suspicious credit card transactions) provide, for practitioners, a fuller picture of possible criminal and terrorist activity. The fragments of digital information that we all leave behind are coming to constitute a crucial new frontier of border security.

The invocation of digital ‘footprints’ and ‘clues’ to explain the way data can be used in the battle against terrorism calls to mind the traces associated with traditional forensic criminal investigation: recoverable impressions, deposits or residues of the body which confer a unique, unassailable identity on every human subject, and which locate relationships between people, places and things in time and space (see Thomas 1994; Williams & Johnson 2008). The forensic trace or clue – whether it is the bloody latent print recovered from a crime scene or profiled DNA body material – is associated with neutrality and facticity, a ‘truth machine’ (Lynch et al. 2008; Cole 2001, 2004) in a duplicitous world. Like the criminal print, the digital footprint appears to provide a neutral ‘mark’ that can direct attention towards suspects. However, while the forensic recovery of the fingerprint or footprint is concerned with piecing together past crimes, with telling a story of ‘what happened here’, the digital footprint has a different temporal orientation. It is not primarily a means of piecing together a criminal or terrorist act after its occurrence, although this is an important aspect of specialist fields of data forensics. Rather, the digital footprint of possible terrorists and criminals allows the anticipation of threatening behaviour before its full materialisation.

In the context of a broad turn to data and analytics within law enforcement, counterterrorism and homeland security (see Adey 2009; Amoore 2006; Amoore & de Goede 2005, 2008a, 2008b; de Goede 2008; Sparke 2006; Valverde & Mopas 2004), the digital footprint combines a concern with ‘evidence’ that cannot help but be left behind in everyday life – ticketing purchases, transaction records, passenger itineraries – with the inference of possible futures. While the comparison of the ‘digital footprint’ with forensic traces is a claim to objectivity and certainty – the simple retrieval of an incriminating trace that was always there – a closer inspection of the history of criminal ‘prints’ reveals a more complex set of concerns, one that resonates closely with the data-led targeting of
contemporary security practice. Bodily prints and metrics have historically been used to try to diagnose a subject’s proclivities *ahead of time*. The original work of the fingerprint, for instance, was not as an investigative clue or as legal evidence. Rather, it was a way of archiving knowledge about criminals by linking bureaucratic records to abstracted biometrics and, more importantly, of identifying risky populations of recidivists and habitual criminals (see Sekula 1986; Cole 2001; Ansorge this issue). The print was an index of the subject’s particularity, but also a way of diagnosing an individual’s disposition, a way of visualising a person’s future capacities before their manifestation.

Similarly, the data print signals an attempt to discern how the traces we leave behind might offer a ‘complete picture of a person’ through which intent might be revealed (Amoore and de Goede 2008a, p. 173; de Goede 2003). For security practitioners, data offers the possibility of inferring intent before its full materialisation as a terror attack or criminal act. For security IT consultants like Detica, the answer is to go beyond matching passengers’ digital footprints against known indicators of risk, or even beyond anomalous, suspicious deviations from ‘normal’ activity. Instead, Detica proposes the *threatprint*: a future digital footprint of a threat not yet in existence. The threatprint approach uses small changes in the data to hypothesise about future threat events and to generate a ‘threat blueprint’ – the not-yet-existing digital footprints these unformed threats would leave. Threatprint style analytics promise to move security practice at the border away from that which is known and verifiable, away from past knowledge, and towards the anticipatory preemption of uncertain futures.

This paper examines the emergence of the digital footprint and the threatprint at the border and its effect within increasingly future-oriented border security practices. Drawing on the history of conventional criminal prints, the paper argues that border targeting systems are little concerned with who we are, in the sense of conventional identity. Data analytics, rather, promises to reveal who we are in the sense of inferring of what we are capable. Like the nineteenth century criminal whose somatic variations gave him or her away in advance, so the mobile subject becomes pre-identified by the traces that are laid down by everyday activity and which come to constitute the important indicator of risk at the border. Data-led targeting appears to offer an objective, factual and incontrovertible method of locating risk, but the targeting of the ‘person of interest’ is always a divisive and potentially discriminatory act. It does not simply divide out a threatening population or subject already constituted. In this way, the data print has much in common with the fingerprint: both are abstractions which simultaneously create and order knowledge about a population and subject yet to fully materialise. The threatprint-style approach to data intelligence creates and recreates potentially suspicious populations at the point of border crossing within a real-time risk assessment which is constantly shifting the parameters of security scrutiny.

**Touchpoints and Travel Cycles**

Edmond Locard, the early pioneer of forensic science, put his name to the field’s core principle of exchange: ‘every contact leaves a trace’. As the criminal body moves through the world, he or she cannot help but leave incriminating impressions and traces of activity. This material, Locard claimed, is a ‘silent witness’: it is ‘[p]hysical evidence [which] cannot be wrong, it cannot perjure itself, it cannot be wholly absent’ (Edmond Locard, cited in Chisum & Turvey 2000). Its apparent facticity gives forensic material a
‘transcendental evidential quality’ which surpasses other types of subjective evidence (Williams & Johnson 2008; Lynch et al. 2008). Retrieved from a crime scene, recovered from a suspect, matched with other traces and deposits, forensic material offers a seemingly incontrovertible method of identifying suspects and of piecing together the facts of a crime.

The two most historically lauded forensic ‘silent witnesses’ – the fingerprint and the DNA profile – locate absolute identifiability in the body’s individuality (see Cole 2004; Sekula 1986; Williams & Johnson 2008), whether this is the distinctive pattern of ridges and whorls on a human digit, or the unique gene variations on an individual’s DNA displayed on a screen, the abstracted bodily trace comes to fix identity and ‘stand for’ the suspect. Cole (2001, 2004) has demonstrated the way in which both the fingerprint and the DNA profile have, in their turn, assumed the status of scientific ‘facts’ in criminal justice systems, despite their problematic position in relation to pure, experimental science (see Lynch et al. 2008). In the early years of the twentieth century, for instance, the fingerprint was referred to as a ‘God-given seal’ – a revolutionary way of individualising bodies (Lynch et al. 2008, p. xii). Nowadays, it is DNA that is the incriminating ‘signature’. Not an impression of the body but actual somatic material, or body-data (Van der Ploeg 2003), the DNA profile confers a gold standard of authority and facticity within criminal investigations (Lynch et al. 2008; M’Charek 2008; Williams & Johnson 2004).

Locard’s principle of ‘every contact leaves a trace’ could equally be applied to the way data residues are imagined within border security initiatives. The UK e-Borders programme, for example, places centrally the passenger’s ‘digital footprint’ created by everyday contact with databased systems via consumption and travel. This footprint is seen as an inadvertent signature of criminal and terrorist activity. The new imperative to gather, share and act on passenger data within systems like e-borders reflects a growing concern to understand not only who is crossing the border, but also what they intend to do. Data encoded in passports (Advanced Passenger Information) is flushed through watchlist databases to identify known suspects before they travel – Is she wanted by the police? Does she have a record? Has she previously claimed asylum? The battle to thwart the unidentified terrorist and the catastrophic attack he or she may be planning, however, requires a data abstraction of passengers that can betray their intent on crossing the border. The Passenger Name Record (PNR) appears to provide this fuller picture.

The PNR is a commercial dataset that the travel industry records on every occasion that someone flies: it might include credit card details for the ticketing purchase, travel agent details, and itineraries for named passengers (see Hobbing 2008, p. 4). The PNR includes a range of data about the passenger and ticket booking from which ‘aspects of the passenger’s history, conduct and behaviour can be deduced’ (House of Lords 2007, p. 9). These fragments, aligned with conventional identity data, give a fuller picture of the mobile person – the credit card that was used to book the ticket, the flight legs that constitute the journey, the passengers’ travel companions. Developed within controversial programmes such as the US Computer-Assisted Passenger Pre-screening System (CAPPs and CAPPs II), as well as the Automated Targeting System for Passengers (ATS-P) and the Transportation Security Administration’s (TSA) troubled new programme, Secure Flight (see EPIC 2007; Hobbing 2008), PNR data has become increasingly significant as a security resource within the international war on terror.

In Europe, existing agreements for the transfer of PNR to the US are being supplemented with plans for a distinct EU PNR system of data capture and sharing.
Subject to numerous redraftings, the EU-PNR proposal as it currently stands will introduce a network of national Passenger Information Units (PIUs), which will receive and process passenger data to carry out ‘real time risk assessment of the passengers’ as well as ‘analysing PNR data for the purpose of identifying trends and patterns . . . to update or create new risk criteria for carrying out risk assessments’ (Council of the European Union 2009, pp. 16, 17). The UK’s e-Borders programme is well ahead of many EU member states. It has a working ‘PIU’ – the National Border Targeting Centre near Manchester Airport – and its use of PNR currently exceeds the EU proposal to use PNR for counter-terrorism and organised crime only (see Home Office 2008, p. 5). In the words of Tom Dodd, Head of UK Border and Visa Policy, e-Borders is an ‘even more sophisticated system’ of border data capture than existing US ones, which focus on a ‘broader range of crime, terrorism and immigration’ (2008). As part of the data footprint of a mobile person, the use of data such as PNR is transforming the border, extending its outward reach and the shadow it casts ‘in-country’.

Recalling the language of customer relations management – where consumers leave valuable clues to their wants, desires and proclivities in their transactions data – the border becomes re-imagined as a series of ‘touchpoints’ within a ‘travel cycle’. Border touchpoints – visa application, ticketing transaction, travel agent booking, airport check-in, passport swipe – are where mobile subjects interface with authorities’ databases (Raytheon 2008). They are also where (potentially incriminating) digital residues are left behind and can be recovered. Airport security, for example, becomes stretched away from the security checkpoint and the border becomes ‘a continuum from the moment somebody makes their reservation until they reach their destination’ (Home Affairs Committee 2010, p. 7). The traces that might betray criminal or terrorist activity are not simply encoded within conventional travel documents, but are to be found within everyday commercial transactions, and so the ‘digital footprint’ is laid down in, and recovered from, a border newly configured, one which is embedded within mundane activity. As Detica outline, the ‘rare event’ of terrorism can be seen as the culmination of a series of ‘mandatory’ actions, processes and interactions embedded within shopping, travel and social behaviour (Agress et al. 2008, p. 171). In this way, the digitised data transaction comes to form the crucial frontier of security knowledge (Amoore & de Goede 2008a): this is the trace that can act as a ‘silent witness’.

Envisaged as a discrete encounter in time and space between a particular mobile body and ‘the border’ which leaves a data trace, the touchpoint is more accurately viewed as the point where security practice gains traction in the mundane necessities of daily living. In this way, the apparently discrete ‘travel cycle’ merges with cycles of consumption, communication and mobility and it is increasingly difficult to trace the border’s limits at all. It is these mandatory actions, which always leave a data residue, which are believed to betray a threat. In the case of the attempted terrorism attack of 25 December 2009 on a flight between Amsterdam and Detroit, for example, it was individual elements of behavior in combination – Umar Farouk Abdulmutallab had paid for his ticket in cash in Ghana, yet started his journey in Nigeria, he was only carrying a book on a two week trip, his visa was issued in the UK despite not travelling through the UK – that, in hindsight, were cited as information that should have been flagged as suspicious (see Home Affairs Committee 2010, ev. 13). It is precisely this kind of data, often retrospectively signalled after an event, that border security programmes like e-Borders are concerned to deploy in advance of an event.
The touchpoint is not simply where the passenger ‘brushes against’ a data capture or retrieval system, but is where a passenger becomes ‘broken up’ or ‘taken apart’ into various transactions, travel itineraries, associations and calculable risk elements (see Amoore & Hall 2009). Like Deleuze’s (1990, p. 6) concept of the ‘dividual’, the subject is partitioned into bits and bytes which become ‘undulatory, in orbit, in a continuous network’ and to which risk scores can be differentially applied. Pixelated data elements are circulated to other touchpoints – recalled at a visa outpost, screened on a border guard’s computer, updated by a passport swipe. It is not simply that the physical body at the border becomes itself a passport through biometric codification (Adey 2009; Amoore 2006; Salter 2006), but rather, ‘imperfect’ forms of identification – appearances, names, documents – become augmented by, even replaced by, more ‘reliable’ identifiers: a lack of luggage, an unusual route, a missed return journey, a cash payment. These abstracted elements offer a way of visualising a subject, of answering the question of ‘what is she doing here?’ The account of the subject demanded at the sovereign border becomes a matter of generating an actionable abstraction from multiple data points.

The discovery of the ‘digital footprint’ or the ‘digital clue’ at the touchpointed border is not the revealing of a coherent and incriminating data object already constituted. Nor is it the piecing together of a surveillant overview of an individual’s movements and activities (see, for example, Weaver & Gahegan 2007). The dream of targeted security is to use rules-based targeting to not focus on licit travellers: to screen out data in order to ‘resource to risk’.¹ The ‘digital footprint’ that security consultants like Detica promise to discover is an recomposition of abstracted elements, an association of data fragments via algorithmic codes and network analysis techniques which bring together individual items of data (this destination with that length of stay, this itinerary with that credit card) and draw relations between them. As Louise Amoore argues, it is precisely the gaps and associations between data items which are vital to producing the picture of threat: it is the ‘multiple decisions about what to select, how to isolate, what should be joined to what’ (2011) that holds together the data dots (a cash payment, an itinerary, a seat choice) which would be meaningless in isolation, but in association become ‘intelligence’ from which a designated action proceeds.

**The Print that ‘Cannot Lie’**

The conventional forensic print gains its authority by its status as settled and coherent ‘object’, divorced from subjective intrusions. The latent fingerprint retrieved from a crime scene, or the DNA material from which a profile is extracted: this is inert evidence that ‘cannot lie’, whose apparently inert materiality constitutes its ‘objectivity’. Forensic science produces apparently authoritative ‘scientific objects’ as ‘objects of evidence’: both, as Latour (2004) argues ‘emphasise the virtues of a disinterested and unprejudiced approach’ (see also Cole 2001; Dror & Cole 2010; Lynch et al. 2008). The forensic trace is factual because it is incapable of being ‘confused by the excitement of the moment’ in Locard’s terms. It appears fixed, immutable. As Daston (1992) argues, objectivity is a historically layered cultural concept, blending notions of ‘asperspectivalism’ (through which the ‘subjectivity of individual idiosyncrasies’ can be overcome), and ‘mechanical objectivity’ (which seeks to eliminate the agency and intervention of the human observers). Objectivity is ‘blind sight, seeing without inference, interpretation, or intelligence’ (Daston & Galison 2007, p. 1). The forensic trace as ‘silent witness’ appears
to offer investigators a ‘blind view’ of a criminal act, a disinterested and impartial abstraction of a past event. Forensic traces must simply be ‘made to speak’ by scientific procedures (M’Charek 2008, p. 521). While of course subject to interpretation, expert authorisation, legal dispute and statistical tests of probability (see Williams & Johnson 2008; Dror & Cole 2010), and notwithstanding the ‘thing-power’ that the forensic object assumes within legal processes (Bennett 2010, see also M’Charek 2008) the forensic trace betrays the suspect (or exonerates her) by appearing to offer incontrovertible immutable facts: this residue came from this person, this fingerprint was left here, this footprint matches this shoe.

The ‘digital print’ of border security is not used to meticulously reconstruct past facts (though data of course offers numerous forensic possibilities after the event). Nor is it a settled and unchanging trace. Rather, the digital footprint as a particular alignment of abstracted data items is responsive and mutable: it is oriented to the question of what should be done here and now. IBM business software analytics, for instance, describe how their predictive data analytics are used to organise vehicle checks along the multiple land border crossings of what is referred to as ‘a large country’ (2010). These analytics draw owner record data and vehicle details (recalled via number plate recognition scans) into association with passport data and crossing histories to select vehicles for searches. Thus, a two-year-old SUV, driven by a man aged 17–24, making a same-day return journey, combined with multiple previous crossings at different checkpoints might give a narcotics risk of 0.75, for instance, and an alert for firearms. The contingencies of local knowledge, and variations in weather, time of day, and day of the week allow a flexible (re)calibration of risk. In the wake of a spate of drugs seizures, for example, a new (previously irrelevant) data trace might be drawn into the calculation and a new abstraction will be used to identify the person warranting extra scrutiny.

The digital footprint, in this way, can hold together new data items, or arrange them in different ways, to give a fresh abstraction and visualisation of a person at the touchpoint. As the risk criteria change, so too does the incriminating print. Concerned with a proactive thwarting of threat, of understanding risk in the here and now, the digital print that identifies threatening activity must constantly be affected by ‘the excitement of the moment’ – new intelligence, fluctuating travel behaviours. While the individual bits of data (a missed flight, a credit card transaction, an unused return ticket, a length of stay) remain static, the algorithmic rules which join them within an abstracted picture of a risky person constantly shift. As one European Commissioner explained in relation to the use PNR: ‘Do you fit the risk level? If not then [your data] will serve a secondary purpose, which is they will give an indication how normal people travel compared to, well, other kind of people’. In this way, the risk criteria at the border touchpoint are not static, but constantly shift and only become ‘self-evident on this particular day at this particular time, at this moment’. For example, the terrorist facilitator David Headley, convicted in the US of the Mumbai attacks, was snared by PNR, which allowed the first name ‘David’, a vague travel window of ‘the next few weeks’ and the partial travel itinerary of a flight from the United States to Germany to become algorithmically targetable. New risk criteria produce new data abstractions, which bring into view new populations and subjects.

The challenge for security analytics is to target efficiently without being overwhelmed by false positives. Understood in Detica’s terms, ‘the relatively small number of digital DNA “markers” that change manifestly between law-abiding citizens and serious criminals’ (Lewis 2008) will always give away threat because they are different. On all sides
of the public debate about data and security practice comes the invocation of ‘good old fashioned police know-how’ and the demand for ‘old-fashioned investigatory work based on evidence and leads, rather than dragnets that treat everyone as suspect’ (ACLU 2007). This search is for a more measured, efficient, ‘humane’ way of fighting crime and terrorism. ACLU (2007) claims that border targeting systems like ATS ‘do not differentiate between evidence and data’ and so direct homeland security resources ‘to wrongly casting a net of suspicion over millions of innocent Americans’. Yet the named individual and the data details of his/her life are not at the centre of security data analytics, despite the public concern around e-borders as a ‘high-tech security blanket’ (Hayes 2009) or with border surveillance as a ‘tightening grip’ and ‘all-encompassing surveillant regime’ (No Borders 2009). The smart border does not want to gather endless data and cast a wide net of suspicion. It wants to target the bytes of information that as part of our abstracted data footprint, designate us as different and worthy of attention: to understand ‘who’s coming into the country and why they’re coming and whether or not you should take action’. It is as concerned with screening out irrelevant data and not targeting licit mobilities as it is with generating intelligence-based leads.

What are the implications of targeting people via their data traces in this way? Certainly the invocation of the ‘footprint’ as inadvertent digital signature of threat occludes the myriad decisions and processes that are intrinsic to its production. The digital footprint is not simply retrieved; rather, it is performative, held together by rules and associations which are developed, in the case of e-borders, by software specialists and border authorities working in close collaboration (see Amoore 2011). For the border guard in an airport, alerted to a screened numeric indicator of risk and an instruction to search for drugs, the multiple decisions and discussions which produced the abstraction of the subject are erased. What is left is a pre-designated course of action following from the representation of the mobile subject via abstracted residues. The possibilities of the subject questioning the visualisation made of them by the traces left behind are few, and the calculative processes through which an abstracted print was generated become lost, even to those acting on them. What emerges, according to border practitioners, is a transactional system that risks transforming active border vigilance into a series of automated responses. The increasing emphasis given to the risk indicators which ‘properly’ identify the mobile subject at the border potentially undermines identification via conventional watchlisting. In June 2011, for example, the Palestinian activist Sheikh Raed Salah was able to enter without hindrance into the UK, despite a travel ban.

Moreover, the shifting nature of the abstracted print which identifies us causes problems for advocacy and civil liberties groups seeking to draw out some of the problems with data-led targeting. Mobilising data protection legislation and privacy rights to counter the production of risk trends and analytical rules derived from personal data conventionally understood (see Amoore 2011) is proving difficult. Liberty (2007, pp. 17–18) for example, notes that e-border data-mining constantly butts against the UK Data Protection Act 1998, but the anonymisation of raw data as well as time limited and targeted use would appear to secure compliance with existing legal requirements. This is often precisely what rules-based targeting and intelligence-led solutions like IBM’s and Detica’s promise. The UK Information Commissioner (2010) similarly calls for ‘striking a balance’ between privacy and security by ensuring proportionality and transparency. Yet when the political debate is mapped out across (albeit vital) issues of redress, transparency and ‘purpose limitation’, the analysis of bits and bytes of dividualised passenger data in an
attempt to produce risk criteria for a targeted approach may start to appear as precisely
the solution that is required.

The analogy of the data ‘footprint’, importantly, appears to rebuff claims that rules-
based targeting might incorporate criteria of race or religion: this is targeting that
proceeds on ‘behaviour not background’, it is claimed (Chertoff 2007), on transactions
rather than appearance. It is an apparently ‘clean’ and objective way of directing security
scrutiny, one which aligns attention with the apparently incontrovertible traces of threat in
emergence. Yet, the digital footprint, we have argued, is an abstraction that constantly
shifts and responds. So, while an orthodox Muslim appearance is not a criteria, patterns of
frequent flights to Pakistan associated with a specific duration of stay may well be. It is not
the case that the digital footprint is a self-evidently incriminating mark, revealed by
analytics. It is an active creation, drawing into focus a constantly shifting population ‘of
interest’ and automating a response to the subject. In this sense it is also difficult to
challenge such programmes under conventional anti-discrimination laws, since they do
not work with criteria that are definitively based on race or ethnicity. Within border
governance programmes like e-Borders, we can see the effort to modulate the uncertain
future which is intrinsic to liberal life (Foucault 2007; see Dean 2007; Rose 1999), become,
via apparently neutral targeting, productive of divisive and exclusionary power relations
that discriminate in new ways. In order that the flows of people, money and objects that
are vital to global order be maintained, some subjects will continually find themselves
targeted in the name of security.

Threatprinting the Future

Conventional forensic traces link a potential suspect to a crime scene, but also
‘generate a suspect where there is none’: first, in the sense of determining the identity of
absent individuals from evidence collected at a crime scene via cold hits with databased
samples; second, by visualising physical characteristics of the unknown suspect (Williams &
Johnson 2008, p. 19; Cole 2004; M’Charek 2008). DNA, particularly, is considered a
‘powerful biological catalogue’ from which it is possible to infer familial links, ‘genetic
ancestry’, ‘ethnic inferences’ and phenotypical features such as eye colour. Although the
fingerprint has been generally discredited as an incontrovertible biometric identifier –
with a ‘match’ between samples now considered a matter of connoisseurship and opinion
rather than absolute scientific certainty (Cole 2008; Dror & Cole 2010) – it originally
promised a rich source of information about the subject.

Francis Galton’s nineteenth century work on finger ridge analysis was originally
concerned not with visualising potential suspects but with organising archival knowledge
of criminals in a context of rapid urbanisation and bureaucratisation (see Cole 2001; Sekula
1986). Galton’s original interest was to locate deviance, risk and threat in biometric facts,
and to understand how human physical variation could indicate a propensity for crime
(Pick 1989, Rabinow 1993). Within a broader eugenic project, the fingerprint, properly
read, would ‘benefit society by detecting rogues’ and would ‘give each human being an
identity ... which can be depended upon with certainty’ (Galton, 1982 cited in Thomas
1994, pp. 659, 660). Galton’s fingerprint was one of several anthropometric devices
used to fix identity within an archive of knowledge and place a given individual within
a population of recidivists and ‘unfit’ habitual criminals, whose propensity for social
menace was written upon their bodies (Sekula 1986). Just as the ‘abnormal’ that Foucault
(2003, p. 20) describes ‘resembles the crime before he has committed it . . .’, so the abstracted inked fingerprint could locate him or her within a population of risk that could be managed ahead of time.

Similarly, ‘digital prints’ are thought to offer a true indicator of proclivity and intent. In the US, justification for ATS blurs potential and actual events, as in the case of the Jordanian Ra’ed al-Banna, who was refused entry to the US in 2003 and later went on to act as a suicide bomber in Iraq in 2005. Stewart Baker (the then Assistant Secretary for Policy at the Department of Homeland Security) commented: ‘No-one knows why al-Banna wanted to enter the US in 2003 — or what he would have done if he’d gotten in. And personally, I’m glad we didn’t get the chance to find out’ (Baker 2006). Here, then, al-Banna’s unknown future — the possible acts he could have committed — formed the basis of an exclusion, the ‘success’ of which emerged afterwards. Indeed, in 2003 the ‘chance to find out’ was precisely what was targeted when the ‘DHS computer system flagged [al-Banna] as someone who ought to get a bit more scrutiny than the usual passenger’ (Baker 2006). The sovereign power to exclude at the border — which has always required evidence of a right to remain, proper documentation, clean health — now increasingly acts upon projected potentialities ‘revealed’ by the data.

What border security data analytics like Detica’s promise, however, is a shift away from established known targets and triggers, or patterns of linked targets and triggers, which provide a ‘thread’ to start pulling on (Detica 2008a, p. 5). It is a focus away from digital footprints used to place subjects into already-identified categories of risk. The cutting edge of data analytics is a move towards ‘threat blueprints’ — or threatprints. Detica describe the threatprint as ‘the set of links between the digital footprints of possible terrorist activities’ (2008b, p. 6): a (speculated) pattern or set of associations between data items that might be used as a diagnostic tool. The threatprint is not a pattern generated via profiles of established criminal or terrorist activity. The threatprint does not attempt to foil a threat already known, or extrapolate forward by applying knowledge of past experience. The threatprint approach directly confronts the uncertainty of the future by projecting a range of future scenarios from which it is possible to look back and ask: What should we have seen in the data? How did the digital clues appear? Whose ‘footprint’ was suspicious? Who should we have searched? As an analytical approach, the threatprint takes anomalous data deviations and then moves one step ahead to hypothesis and envisage possible future events that have yet to happen. The threatprint directs the search for evidence as if the future threat event had already happened.

In the casting forward of ‘projected lines of sight’ (Amoore 2009) in this way, data analysis speculatively produces certain kinds of future. Grusin’s (2004) description of premediation is useful here. Premediation is the proliferation of endless potential future scenarios that may or may not be probable, and which may or may not come to fruition. The threatprint is one such premediated element, it ‘makes the future present’, bringing into presence something that has not yet, or may never happen (see Massumi 2005, 2007). The point is not to precisely predict what will happen based on induction from past events, but to generate a ‘constant readiness to identify another possible way in which a radically different future may play out’ (Anderson 2010, p. 782; see Amoore 2011). This style of data analytics seeks to break future (possible, probable and improbable) threat events into ‘component parts’ so the first traces of a threat in emergence may be identified as it starts to materialise in the data: an apparently innocent journey, a certain
pattern of consumption, a particular ticketing transaction, producing ‘large repositories of threatprints . . . for many types of security threat’ (Detica 2008b, p. 6). The threatprint points to an anticipatory form of governance at the border that pushes beyond triggers and targets of suspicious activity already identified, towards the analysis of a print that unknown threat disseminates ahead of itself.

The threatprint, then, moves security practice away from ‘reality-based’ evidence (see Suskind 2004). It alters what Jonas (2007) calls the ‘predicates’ upon which security investigations and inspections proceed. In searching for the print that threat is already leaving ahead of itself, no scenario has been overlooked. The threatprinted future and the appropriate calculated response become co-generated. In making the prints of potential futures the basis of security practice – of determining the targets and triggers for scrutiny, locating the anomaly for secondary screening – a person might be targeted not because their data footprint is self-evidently suspicious and not because it matches with a pattern or risk profile for established threatening activity or deviates from an existing norm. Rather, a person may be targeted because the pattern of activity described by the data matches with the prints cast back from a projected future. Like Galton’s nineteenth century criminals – whose bodies leave prints which indicate their proclivities – the futures of ‘persons of interest’ have already been imagined, traces of their future actions are already being left behind.

‘The Future Ain’t What it Used to Be’

Increasingly, then, the urge to ‘stay ahead of the digital wave’, to ‘move from chasing threats to anticipating them well ahead of time’ to ‘predict and act’ rather than ‘sense and respond’ (see IBM 2010) make speculative ‘what ifs’ the ‘inevitable future’ (Elmer & Opel 2006). It scarcely matters whether an attack actually takes place, or whether a scenario corresponds to future reality. It is fear, according to Massumi (2005), which operates as a mechanism of linkage between future threat and its capacity to affect the here and now. As Melinda Cooper (2008) argues, the preemptive strike founds the legitimate use of violence on a fearful ‘collective apprehension of the future’ rather than a ‘predictive calculus of risk’. Increasingly, as Amoore (2011) argues, action in the face of uncertainty becomes more important than the occurrence of specific events. Preemption differs from other future oriented logics such as preparedness and precaution (see Anderson 2010). Precaution, for instance, ‘advises on a course of absolute intolerance to the future’ (Cooper 2008, p. 89), but key to preemption, for Massumi (2005, p. 8), is the way it effects and ‘induces the event’: ‘It makes present the future consequences of an eventuality that may or may not occur, indifferent to its actual occurrence. The event’s consequences precede it’. Preemption involves immersion in the conditions of emergence of the future ‘to the point of actualising it ourselves’ (Cooper 2008, p. 89). The desire to intervene ‘before the terrorist or criminal has been radicalised or recruited in the first place’ (Detica 2008a) is not a response to a threat, but the co-creation of a future.

In this way, we can see that the political technologies of security practice at the border rely upon a laissez-faire approach to mobility, uncertainty and contingency, one which Foucault (2007) describes as the modulating of uncertain outcomes rather than governing via a disciplinary norm. The very uncertainty and contingency of life within liberalism is the problem and the solution (see Anderson 2010). At the border, the multiple crossings of money, bodies and objects must be maintained at their frenetic pace, and the
constant movement will provide, via the data, the key to securing their passage because
the threat can be targeted before its emergence. In the security sectors there is, then, a
growing awareness that ‘the emergent behaviour of the system as a whole is extremely
difficult to predict from the characteristics and relationships of the system elements’
(Moffat 2003, p. 3). For William Connolly (2004, p. 342), a critical response should
*naturalize a place for mystery, folding a modicum of it into emergent causality’, which he
describes as the “uncertainty” [that] exceeds the assumption of limited information
marking conventional empiricist and rational choice theories’. The turn to data, however,
signals a mode of governance which works with, and acts upon, the possibility of mystery,
and which aims to preempt future events before their full materialisation.

The modes of governance at work in programmes like e-Borders, then, seek to
intervene against emergent factors, the everyday activity that, in retrospect, forms the
‘mandatory steps’ towards the threat event. This is not a preventative or disciplinary mode
of governing in Foucault’s terms (2007). It does not seek to inculcate a mode of ‘proper’
travel behaviour, nor close down the future. The threatprint approach signals an attempt
to capture the outline of ‘non-conceptualisable’ emergent factors, the unknown
unknowns – and counter these threats prior to their emergence into a catastrophe.
People like al-Banna are targeted before they can engage in the action they are being
targeted for. The simulations of security that the threatprint mobilises are not really
concerned with what is probable, but with *actualising* a hyperreality so the rare threat
event has always already happened and been countered. Here we might turn to Massumi’s
description of the potentiality of the virtual as:

[T]he future-past of the present: a thing’s destiny and condition of existence . . . The
virtual is real and in reciprocal presupposition with the actual, but does not exist even to
the extent that the actual could be said to exist. It *subsists* in the actual or is immanent to
it. (1992, pp. 36–37)

Like Galton’s nineteenth century criminals – whose bodies contained indications of their
futures and proclivities – the future pasts of ‘persons of interest’ might already be leaving
traces in the data record, if only the software could reveal them. In the abstraction and
visualisation of the ‘person of interest’, the possibility of other, unknown, futures –
keeping open a space for contingency – become folded into the threatprint. These
tries to capture the future mean that a ‘terrorist’ or ‘criminal’ is made the target of
suspicion well ahead of any actual crime. It is, thus, indeed the case that (as Yogi Berra
once put it) ‘the future ain’t what it used to be’. There is a violence connected to this,
which is ‘akin to the “dark matter” of physics’ (Žižek 2008, p. 2): it rests not on the brutality
of violent acts of terror or crime, but on the very intervention upon future potential.
The future is no longer an open space of potential. Instead, preemptive politics that take
place in Massumi’s future past of the present (1992, pp. 36–37) are already imagined to
have subsumed the future and its surprises. As the future past of the present collapses into
the now, the virtual no longer offers a space of possibility, but now swallows up what
might once have been future potential.

In many ways, then, there is a shift from Deleuzean to Baudrillardian simulation and
virtuality, from virtuality as potential to virtuality as simulation (see Baudrillard 1994):
performing and simulating a type of counter-terrorist activity, projecting realities with real
(potentially violent) effects. For Deleuze, the simulacrum ‘is not degraded copy, rather it
contains a positive power which negates both original and copy, both model and
reproduction’ (1983, p. 53). However, the productivity of the space between tracing discernible changes in the data and the production of targets and triggers from projected threatprints is not a positive power: it destroys future potentials, as future possible scenarios become reduced to more Baudrillardian simulations. There are attempts to close down the potential and indeterminacy of the Deleuzean virtual: a virtual which is ‘called virtual in so far as their emission and absorption, creation and destruction, occur in a period of time shorter than the shortest continuous period imaginable; it is this very brevity that keeps them subject to a principle of uncertainty or indetermination’ (Deleuze & Parnet 2002, p. 148).

Yet contemporary simulation ‘has weakened, in some cases displaced, and in others completely redrawn, the representational boundary between the simulation and the “real thing”’ (Der Derian 2001, p. 194). For Baudrillard, famously, the distinction between reality and signs dissolves within simulation (1988). Simulation is not a matter of pretence, of feigned imitation, but ‘of substituting signs of the real for the real itself . . .’: ‘simulation threatens the difference between “true” and “false”, between “real” and “imaginary”’ (Baudrillard 1988, pp. 167–168). Within the hyperreality that is produced by simulation, ‘origins are forgotten, referents lost, and simulations begin to precede and engender reality’ (Der Derian 2001, p. 194). Threatprints, then, generate prints or traces of simulated future threat, actualising a hyperreality so the rare threat event has always already happened and been countered. The threatprint governs the uncertain future not only by seeking to visualise unknown unknowns, but by virtualising them so that all outcomes have already been produced and preempted. The ‘could have/would have’ logic of these conditional politics can never be falsifiable: only subject to more refined adjustments. Simulation here is thus not an opening up of potential, but of collapsing future potentials into the recoverable marks that are already being inadvertently left.

What kind of population is being targeted here? The threatprint acts as a device that claims to simply represent or target a population already constituted via their abstracted data. Yet the constant realignment of risk and the production of fresh data abstractions produce endlessly refinable targets of interest that may never fully emerge. Here we might return to the organisation of nineteenth century knowledge around the habitual criminal population. Far from constituting a latent category, this group was ‘made up’ (Hacking 1990) via metric approaches to the body to differentiate between ‘types’ of offender and normal citizenry. The digital print of contemporary border security also ‘makes up’ specific populations of risk, dividing the undesirable from the desirable in real time and ahead of time, orienting security attention in the moment to a specific population. The organisation of attention via the threatprint allocates risk to an abstraction brought into focus from a future that may never come. It takes the evidence that cannot help but be left behind, and compares it with the traces that an unformed threat would leave. How, then, could a person called aside for airport questioning for instance, ever know the circumstances and reasons for this scrutiny? How could a subject ever explain a digital footprint that misrepresented him or her?

Conclusion

The data war that is fought in the name of counter-terror in Europe and beyond is concerned to mobilise the uncertain future to pre-empt the next attack and intervene ‘before the terrorist has been radicalised’. Embodied within border targeting systems like
e-borders, the dream to strike ahead of time – to modulate the course of the future and annul the surprise catastrophic event – works through the data abstractions, or ‘footprints’, that have become an inevitable feature of contemporary life. The security consultants’ ‘rules-based targeting’ and ‘intelligence-led approach’ is frequently cited as the ‘solution’ to the proliferation of data. The digital footprint and the threatprint approach promise a way of not focusing on millions of innocent, normal journeys, in contrast to the public concern around border surveillance. The ‘digital footprint’, it is argued, is a reliable way of directing attention, of bringing into focus risky activity, combining technical capability with ‘old-fashioned’ investigative techniques. Yet the frequent comparison with the prints and traces of forensic practice is not as straightforward as it first appears. The digital print has less in common with the criminal print as objective evidence of past events and more in common with the projected futures of Francis Galton’s criminal anthropometry. It is by exposing what is hidden by such analogies that the effects of the data footprint can be grasped.

Relatively unconcerned with the details of ‘what has gone before’, the digital print is an abstraction from which an identification can be made and a response can be calculated. Yet this is not a clean and objective strike, but one which encodes decisions and associations within algorithmic rules to produce a screened resolution and action from which these decisions are erased. It is important here to note that the ‘silent witness’ of forensic practice is also an active creation. The screened ‘stripes and peaks’ of the DNA profile, for example, occlude its performative power as an unstable network of relations, which draws together norms, goals, assumptions and omissions: it is an ‘articulate collective’ rather than a ‘silent witness’ (M’Charek 2008, p. 523). In border security, the ‘ping’ against the rules, as practitioners term it, seems to be a simple match between recovered data traces and reliable indicators of risk. More accurately, though, the shifting and unstable risk calibrations produce new data associations, new abstractions and new visualisations. The abstracted data ‘footprint’ that identifies me does not seek to piece together what I have done, but calculates what risk I might pose now. The violence of the targeting lies not only in the action that follows (question, detain, search), but in the claim to have definitely identified a person via the bits and bytes left behind. Increasingly, we have argued, the violence ‘akin to the “dark matter” of physics’ (Žižek 2008, p. 2) lies in the willingness to proceed towards the uncertain future by deploying threatprint-style scenarios as the predicates against which security action proceeds. The (vital) critical lenses provided by those defending civil liberties and privacy struggle to visualise this dark matter when new questions abound about who is harmed, what is to be protected and what there is to defend. Against visions of the ‘clean’ preemptive strike we would highlight the presence of this dark matter: actions against projected futures and the creation of targetable populations that have yet to fully emerge.

The fingerprint, Francis Galton originally believed, would be able to detect criminals who were pretending to be someone they were not (Galton cited in Thomas 1994, p. 667), rather like the contemporary terrorist who ‘hides in plain sight’ (Jonas & Harper 2006). Galton’s great expectation was that the print could determine the ‘true identity’ of a person in the sense of diagnosing in advance, and with certainty, a person’s latent disposition (Rabinow 1993, p. 59; Thomas 1994, p. 667). Galton’s lasting regret, argues Rabinow (1993), was that these expectations were unfounded. The print gave no reliable indication of proclivity for criminality at all, despite clusters of similarities within certain population groups (see Cole 2001). Just as Galton’s metrics of the criminal body which strove to
decipher its latent threat proved unsuccessful, so current efforts to intervene on potential futures and trace out possible threat through the data traces it disseminates ahead of itself constantly confront the potentialities of human life that will always exceed what can be ‘held’ or ‘captured’ within the threatprint. For Melinda Cooper (2008, p. 99), a counter politics to the doctrine of preemption must attempt to ‘undermine the foregone conclusion’. This paper has shown that it is precisely the foregone conclusion that is animating the turn to data within the war on terror. It is by demonstrating the contingency of the apparently authoritative data-led ‘finger of suspicion’ that our ‘foregone identification’ can begin to be undermined.

ACKNOWLEDGEMENTS

This paper emerged from collaborative work of the ESRC-NWO funded project Data Wars: New Spaces of Governing in the War on Terror, RES-062 230594 led by Professor Louise Amoore and Professor Marieke de Goede. This paper was presented at the Critical Geopolitics conference, Durham University, September 2008 and also at the Data Wars workshop, University of Amsterdam, June 2009 and the CRESC Annual Workshop, September 2009. Thanks to Louise Amoore, Marieke de Goede, Mara Wesseling for their comments on this paper, and to conference participants for their feedback. Thanks also to the contributions and comments from the anonymous reviewers.

NOTES

1. Interview with e-borders official, London, March 2009.
2. Interview with European Commissioner at Directorate-General Justice, Freedom and Security, Brussels, April 2009.
3. Interview with e-borders official, London, March 2009.
4. Interview with private border security consultants, London, March 2009.

REFERENCES

ADEY, P. (2009) ‘Facing airport security: Affect, biopolitics, and the preemptive securitisation of the mobile body’, Environment and Planning D, Society and Space, vol. 27, no. 2, pp. 274–295.

AGRESS, R. CHRISTIANSON, A., NICHOLS, B., & PORTER, D. (2008) ‘The case for use of a multi-method scientific approach for anticipating a rare event’, in Anticipating Rare Events (Topical Strategic Multi-Layer Assessment Multi-agency/Multi-disciplinary white papers in support of counter-terrorism and counter WMD), Homeland Security Digital Library, [Online] Available at: https://www.hsdl.org (accessed 11 July 2011).

AMERICAN CIVIL LIBERTIES UNION (ACLU). (2007) ACLU Backgrounder on ATS, [Online] Available at: http://www.aclu.org/technology-and-liberty/aclu-backgrounder-ats (accessed 11 July 2011).

AMOORE, L. (2006) ‘Biometric borders: governing mobilities in the war on terror’, Political Geography, vol. 25, pp. 336–51.

AMOORE, L. (2009) ‘Lines of sight: on the visualisation of unknown futures’, Citizenship Studies, vol. 13, no. 1, pp. 17–30.
AMOORE, L. (2011) ‘Data derivatives: on the emergence of a security risk calculus for our times’, *Theory, Culture and Society*, vol. 28, pp. 3–23.

AMOORE, L. & DE GOEDE, M. (2005) ‘Governance, risk and dataveillance in the war on terror’, *Crime, Law and Social Change*, vol. 43, no. 2, pp. 149–173.

AMOORE, L. & DE GOEDE, M. (2008a) ‘Transactions after 9/11: the banal face of the preemptive strike’, *Transactions of the Institute of British Geographers*, vol. 33, no. 2, pp. 173–185.

AMOORE, L. & DE GOEDE, M. (2008b) ‘Introduction: Governing by risk in the war on terror’, in *Risk and the War on Terror*, eds L. Amoore & M. de Goede, Routledge, London, pp. 5–21.

AMOORE, L. & HALL, A. (2009) ‘Taking people apart: digitised dissection and the body at the border’, *Environment and Planning D: Society and Space*, vol. 27, no. 3, pp. 444–464.

ANDERSON, B. (2010) ‘Preemption, precaution, preparedness: anticipatory action and the future’, *Progress in Human Geography*, vol. 34, no. 6, pp. 777–798.

BAKER, S. (2006) ‘Remarks of Stewart Baker, Assistant Secretary for Policy, Department of Homeland Security at the Center for Strategic and International Studies, Washington, DC’, [Online] Available at: http://www.dhs.gov/xnews/speeches/sp_116655796765.shtm (accessed 26 February 2009).

BAUDRILLARD, J. (1988). Jean Baudrillard. Selected Writings, Stanford University Press, Cambridge.

BAUDRILLARD, J. (1994) *Simulacra and Simulation*, University of Michigan Press, Ann Arbor.

BENNETT, J. (2010) *Vibrant Matter: A Political Ecology of Things*, Duke University Press, Durham, NC.

CHERTOFF, M. (2007) ‘Speech delivered to the Committee on Justice, Civil Liberties and Home Affairs, European Parliament, 15 May’, [Online] Available at: http://www.dhs.gov/xnews/speeches/sp_1180627041914.shtm (accessed 12 July 2011).

CHISUM, W. J. & TURVEY, B. (2000) ‘Evidence dynamics: Locard’s exchange principle and crime reconstruction’, *Journal of Behavioral Profiling*, vol. 1, no. 1.

COLE, S. (2001) *Suspect Identities: A History of Fingerprinting and Criminal Investigation*, Harvard University Press, Cambridge, MA.

COLE, S. (2004) ‘Fingerprint identification and the criminal justice system: historical lessons for the DNA debate’, in *DNA and the Criminal Justice System: The Technology of Justice*, ed. D. Lazer, MIT Press, Cambridge, MA, pp. 63–89.

COLE, S. (2008) ‘The “opinionization” of fingerprint evidence’, *BioSocieties*, vol. 3, no. 1, pp. 105–113.

CONNOLLY, W. E. (2004) ‘Method, problem, faith’, in *Problems and Methods in the Study of Politics*, eds I. Shapiro, R. M. Smith & T. E. Masoud, Cambridge University Press, Cambridge, pp. 332–349.

COOPER, M. (2008) *Life as Surplus: Biotechnology and Capitalism in the Neoliberal Era*, University of Washington Press, Seattle.

COUNCIL OF THE EUROPEAN UNION. (2009) Note from the Presidency to the Multidisciplinary Group on Organised Crime (5618/2/09), [Online] Available at: http://www.statewatch.org/news/2009/jul/eu-ctrl-council-5618-rev2-09.pdf (accessed 11 July 2011).

DASTON, L. (1992) ‘Objectivity and the escape from perspective’, *Social Studies of Science*, vol. 22, pp. 597–618.

DASTON, L. & GALISON, P. (2007) *Objectivity*, Zone Books, London.

DE GOEDE, M. (2003) ‘Hawala discourses and the war on terrorist finance’, *Environment and Planning D: Society and Space*, vol. 21, no. 5, pp. 513–532.

DE GOEDE, M. (2008a) ‘The politics of preemption and the war on terror in Europe’, *European Journal of International Relations*, vol. 14, no. 1, pp. 161–185.

DEAN, M. (2007) *Governing Societies*, Sage, London.
DELEUZE, G. (1983) ‘Plato and the simulacrum’, October, vol. 27, pp. 45–56.
DELEUZE, G. (1990) ‘Postscript on the societies of control,’ October, vol. 59, Winter, pp. 3–7.
DELEUZE, G. & PARNET, C. (2002) ‘The actual and the virtual’, Dialogues II, Continuum, London and New York, pp. 148–152.
DER DERIAN, J. (2001) Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network, Westview Press, Colorado.
DETICA. (2008a). The Information Revolution and its Impact on Homeland Security, [Online] Available at: http://www.detica.com/images/pdfs/detica_information_revolution_whitepaper.pdf (accessed 26 February 2009).
DETICA. (2008b) ‘The new front line: exploiting the digital revolution to improve our response to the terrorist threat’, [Online] Available at: http://www.detica.com/the-new-front-line.html (accessed 12 July 2011).
DODD, T. (2008) ‘Evidence given before House of Lords European Union Committee.’ In The Passenger Name Record (PNR) Framework Decision, 15th Report of Session 2007–2008, House of Lords European Union Committee, The Stationery Office Limited, London.
DROR, I. & COLE, S. (2010) ‘The vision in “blind” justice: expert perception, judgment, and visual cognition in forensic pattern recognition’, Psychonomic Bulletin and Review, vol. 17, no. 2, pp. 161–167.
ELECTRONIC PRIVACY INFORMATION CENTRE (EPIC). (2007) EU-US Airline Passenger Data Disclosure, EPIC, Washington DC, [Online] Available at: http://epic.org/privacy/intl/passenger_data.html (accessed 12 July 2011).
ELMER, G. & OPEL, A. (2006) ‘Surviving the inevitable future: pre-emption in an age of faulty intelligence’, Cultural Studies, vol. 20, nos 4–5, pp. 477–492.
FOUCAULT, M. (2003) Abnormal: Lectures at the Collège de France 1974–1975, tr. G Burchell, Macmillan, Basingstoke.
FOUCAULT, M. (2007) Security, Territory, Population: Lectures at the Collège de France 1977–1978, tr. G Burchell, Macmillan, Basingstoke.
GRUSIN, R. (2004) ‘Premediation’, Criticism, vol. 46, pp. 17–39.
HACKING, I. (1990) The Taming of Chance. Cambridge University Press, Cambridge.
HAYES, B. (2009) Neoconoption: The EU Security-Industrial Complex, Statewatch, London.
HOBBING, P. (2008) Tracing Terrorists: The EU-Canada Agreement in PNR Matters. Centre for European Policy Studies Special Report, [Online] Available at: www.ceps.eu (accessed 12 July 2011).
HOME OFFICE. (2008). Code of Practice on the Management of Information Shared by the Border and Immigration Agency, HMRC and the Police, [Online] Available at: http://www.ukba.homeoffice.gov.uk/sitecontent/documents/managingourborders/eborders/codeofpractice/ (accessed 12 July 2011).
HOUSE OF COMMONS. (2010) ‘Counter-Terrorism Measures in British Airports’, Ninth Report of Session 2009–2010, Home Affairs State Select Committee, The Stationery Office Limited, London.
HOUSE OF LORDS. (2007) ‘The EU/US Passenger Name Record (PNR) Agreement’, 21st Report of Session 2006–2007, European Union Committee, The Stationery Office Limited, London.
IBM. (2010) Public Safety: From ‘Sense and Respond’ to ‘Predict and Act’, IBM Corporation, New York.
INFORMATION COMMISSIONER’S OFFICE. (2010) Information Commissioner’s Report to Parliament on the State of Surveillance, UK Information Commissioner’s Office, Wilmslow.
JONAS, J. (2007) *Predicate-based Link Analysis: A Post 9/11 Analysis (1+1 = 13)*, [Online] Available at: http://jeffjonas.typepad.com/jeff_jonas/2007/04/predicatebased_.html (accessed 12 July 2011).

JONAS, J. & HARPER, J. (2006) *Effective Counterterrorism and the Limited Role of Predictive Data Mining, Policy Analysis No. 584*, Cato Institute, Washington DC.

LATOUR, B. (2004) ‘Scientific objects and legal objectivity’, in *Law, Anthropology and the Constitution of the Social*, eds A. Pottage & M. Mundy, Cambridge University Press, Cambridge, pp. 73–114.

LEWIS, H. (2008) ‘Threatprints — Digital DNA criminals leave behind’, *Contingency Today*, [Online] Available at: http://www.contingencytoday.com/online_article/Threatprints—digital-DNA-criminals-leave-behind/-1620 (accessed 12 July 2011).

LIBERTY. (2007) *Overlooked: Surveillance and Personal Privacy in Modern Britain*, [Online] Available at: http://www.liberty-human-rights.org.uk/issues/3-privacy/pdfs/liberty-privacy-report.pdf (accessed 12 July 2011).

LYNCH, M., COLE, S., MCNALLY, R. & JORDAN, K. (2008) *Truth Machine: The Contentious History of DNA Fingerprinting*, Harvard University Press, Cambridge, MA.

M’CHAREK, A. (2008) ‘Silent witness, articulate collective: DNA evidence and the inference of visible traits’, *Bioethics*, vol. 22, no. 9, pp. 518–528.

MASSUMI, B. (1992) *A User’s Guide to Capitalism and Schizophrenia: Deviations from Deleuze and Guattari*, The MIT Press, Cambridge, MA.

MASSUMI, B. (2005) ‘The future birth of the affective act. Conference proceedings: Genealogies of Biopolitics’, [Online] Available at: http://browse.reticular.info/text/colllected/massumi.pdf (accessed 13 July 2011).

MASSUMI, B. (2007) ‘Potential politics and the primacy of preemption’, *Theory and Event*, vol. 10, no. 2.

MOFFAT, J. (2003) *Complexity Theory and Network Centric Warfare*, DoD Command and Control Research Program, Washington, DC.

NO BORDERS. (2009) *E-borders: The Tightening Grip of the Border Regime*, [Online] Available at: http://noborderswales.org.uk/2009/04/22/e-borders-the-tightening-grip-of-the-border-regime. (accessed 12 July 2011).

PICK, D. (1989) *Faces of Degeneration: A European Disorder, c.1848–c.1918*, Cambridge University Press, Cambridge.

RABINOW, P. (1993) ‘Galton’s regret and DNA typing’, *Culture, Medicine and Psychiatry*, vol. 17, pp. 59–65.

RAYTHEON. (2008) Unpublished presentation made at the Homeland and Border Security Conference 2008: *Working Together, Securing the Nation*, 3 July 2008, QE11 Conference Centre, London.

ROSE, N. (1999) *Powers of Freedom: Reframing Political Thought*, Cambridge University Press, Cambridge.

SALTER, M. (2006) ‘The global visa regime and the political technologies of the international self: borders, bodies, biopolitics’, *Alternatives*, vol. 31, pp. 167–189.

SEKULA, A. (1986) ‘The body and the archive’, *October*, vol. 39, pp. 3–64.

SPARKE, M. (2006) ‘A neoliberal nexus: economy, security and the biopolitics of citizenship on the border’, *Political Geography*, vol. 25, pp. 151–180.

SUSKIND, R. (2004). ‘Faith, certainty and the presidency of George W. Bush’, *The New York Times*, [Online] Available at: http://www.nytimes.com/2004/10/17/magazine/17BUSH.html?ex=
THOMAS, R. (1994) ‘The fingerprint of the foreigner: colonising the criminal body in 1890s
detective fiction and criminal anthropology’, *ELH*, vol. 61, no. 3, pp. 655–683.
VALVERDE, M. & MOPAS, M. (2004) ‘Insecurity and the dream of targeted governance’, in *Global
Governmentality: Governing International Spaces*, eds W. Larner & W. Walters, Routledge,
New York, pp. 233–250.
VAN DER PLOEG, I. (2003) ‘Biometrics and the body as information: normative issues of the socio-
technical coding of the body’, in *Surveillance as Social Sorting*, ed. D. Lyon, Routledge,
London, pp. 57–75.
WEAVER, S. D. & GAHEGAN, M. (2007) ‘Constructing, visualising and analysing a digital footprint’,
*Geographical Review*, vol. 97, pp. 324–350.
WILLIAMS, R. & JOHNSON, P. (2004) ‘Wonderment and dread: Representations of DNA in ethical
disputes about forensic DNA databases’, *New Genetics and Society*, vol. 23, no. 2,
pp. 205–223.
WILLIAMS, R. & JOHNSON, P. (2008) *Genetic Policing: The Use of DNA Profiling in Criminal
Investigations*, Willan Publishing, Cullumpton.
ŽIŽEK, S. (2008) *Violence*, Profile Books, London.