## Security and the claim to privacy

When US President Barack Obama addressed the data mining and analysis activities of the National Security Agency he appealed to a familiar sense of the weighing of the countervailing forces of security and privacy. “The people at the NSA don’t have an interest in doing anything other than making sure that where we can prevent a terrorist attack, where we can get information ahead of time, we can carry out that critical task”, he stated. “Others may have different ideas”, he suggested, about the balance between “the information we can get” and the “encroachments on privacy” that might be incurred (Obama 2013). In many ways conventional calculations of security weigh the probability and likelihood of a future threat on the basis of information gathered on a distribution of events in the past. Obama’s sense of a trading off of security and privacy shares this vocabulary of probabilities – of a calculation of the tolerance for the gathering of data on past events in order to prevent threats in the future. Curiously, though, the very NSA programmes he is addressing here precisely confound the weighing of probability, and the conventions of security and privacy that adhere to strict probabilistic reasoning. The contemporary mining and analysis of data for security purposes invites novel forms of inferential reasoning such that even the least probable elements can be incorporated and acted upon. These elements of possible associations, links and threats do not meaningfully belong to an identifiable subject as such, much less belong to a data subject with a recognisable body of rights to privacy, to liberty, to justice.

Consider, for example, two years before the controversies surrounding NSA and the PRISM programme, when the US Director of National Intelligence James Clapper testifies before the joint hearing of committees on the virtues of the algorithmic piecing together of fragments of data:

> The most valuable national intelligence is the huge collection of databases of routinely collected information that can be searched by computer algorithm. An analyst may know that a *potential* terrorist attacker is between 23 and 28 years old, has lived in Atlanta Georgia, and has travelled often to Yemen. That analyst would like to be able to very rapidly query the travel records, the customs and border protection service, the investigative records of the State Department […] we made important progress after the December 2009 attempted bombing of an aircraft over Detroit, but there remains much more to be done (US Senate Committee 2011: 16).

What is sought in the director of the DNI’s vision is not the probable relationship between data on past activities and a future terrorist attack, but more specifically a *potential* terrorist, a subject who is not yet fully in view, who may be unnamed and as yet unrecognisable. The security action takes place on the terrain of a potential future on the horizon, a future that can only be glimpsed through the plural relations among data points.

Now, why does a security of fragments and potentials matter to our sense of privacy, both as a concept and as a body of rights? In a form of security wrought via the assembly of data elements it is not the aim to collect a complete file of information on

a person, indeed incompleteness is a virtue. In the public debate the talk of 'metadata' imagines that the spoken content of a telephone conversation is private data, whilst the call number, location, time of call and so on is 'meta'. In fact, though, it is the derivative meta-data of associative links between elements that are the valuable data points for social network analysis. In a sense, the 'content' of the "dots to be connected" matters less to this kind of analysis than the relations between them. The absence of a complete record thus becomes a security virtue because it makes it more difficult to assume that content is 'innocent' – in effect, apparently innocent content can become suspicious because it is subsequently associated with other things. But of course while 'content' appears readily identifiable with a subject, the meta-data of links among multiple people and things, and among multiple parts of a subject are indifferent to the person as such. The individual who is the subject of privacy rights, and the data subject of data protection, is differently rendered in this mode of security. In the anticipatory analysis of data one does not need to know who someone is – at least not in the conventions of identification – but what they mean in relation to an array of possible associations.

Put simply, contemporary forms of security are less interested in who a suspect might be than in what a future suspect may become, less interested in the one-to-one match of the watch list or alerts index database, and more interested in the signals of real-time predictive analytics. The one-to-one match with an individual gives way to what Gilles Deleuze called the "dividual" – a "torn chain of variables" dividing the subject within herself, recombining with the divided elements of others (1992: 3). The signature of the dividual that is sought by the security software does not 'belong' to a subject as such – it does not sign off on past events, it signals possibilities. Thus, for example, an agreement to 'depersonalize' data in a database after a period of six months, as in the case of the EU-US agreement on passenger name record (PNR) data scarcely matters when what is left is a dividuated signature that allows for the writing of new code. So, a subject's specific and named journey on a particular date may no longer be attributable in the database, but it persists as a source for new algorithmic code to act on future subjects.

Some dividuated data elements are disaggregated from the remainder and become drawn into association with other elements derived from other subjects. This has significance even in the conventional debates about the analysis of data making us more secure. For example, the 2009 New York subway suspect Najibullah Zazi, the 2009 Northwest Airlines Detroit bomber Umar Farouk Abdulmutallab, and the 2010 Times Square bomber Faisal Shahzad could be offered as examples of the fallibility of a system of risk-based data analysis. Yet, though none of the suspects was pre-emptively intercepted on the basis of the analysis of their travel or financial data, the fragments of data did reappear as a chain of variables for future algorithmic searches. In the analysis of the US Attorney General, they had ceased to be identifiable subjects and had emerged as "operatives with British or American passports or visas who had visited South Asia and had returned to the US over (redacted) time period" (2011: 4). It is the chain of variables of their data fragments that live on in contemporary border security analytics.

If the subject of contemporary security measures is a fractionated subject whose missing elements are a resource to analytics technologies, then *can we meaningfully conceive of a right to privacy of the dividual?* Such a form of privacy would adhere

not to identifiable individuals but to the associations and links between multiple pieces of multiple people's lives. If what is collected, analysed, deployed and actioned in contemporary security is not strictly personal data elements, but what I have elsewhere called a 'data derivative' – a specific form of abstraction like a financial derivative, that can have value that is decoupled or only loosely tied to its underlying coordinate – can privacy have meaningful purchase on this slippery derivative? One response has been to seek to restrict the use of personal data and to assert the right to be deleted or forgotten (Mayer-Schönberger 2009). But the data derivative makes associations and links that will always exceed a specified use, will travel and circulate with new effects and implications. Because the fragments of data are unmoored from specific underlying content they evade jurisdiction that requires an individual body or body politic.

So, *what might it mean to have data protection*, or to limit use to defined purpose in a world of abstracted data signatures? The gathering of evidence of terrorist activities after the fact is seeping into the pre-emptive search for indicators of intent capable of anticipating future possible infraction. In this sense, for example, what is significant about the UK's GCHQ generating 197 leads from PRISM in 2012 is not the 197 but how the 197are arrived at. The 197 represent persons of interest that have come to attention after a process of running large volumes of data through the predictive analytics software. It is the analytics that govern what the elements of interest should be – this travel associated with this financial transaction, associated with this presence in an open source online community, associated with this presence on Facebook, for example. So, put simply, the vast bulk of the filtering and analysis happens before any named individuals or lists are identified. It is not strictly the privacy of the individual that is infringed by programmes such as PRISM, but the harm is in the violence done to associational life, to the potentiality of futures that are as yet unknowable (de Goede 2012). In effect the data do not have meaning until sense is made of them by the relational structure of the analytics. One could protect data very effectively and yet still the inferred meanings of the analytics would limit life chances and close down potential futures.

Perhaps the most significant harm, though, lies in the violence done to politics itself, and to the capacity to make a political claim. Where politics exists because of intractability and irresolvability, because of difficulty as Thomas Keenan (1997) puts it, contemporary data-led security offers resolution through computation, promising to resolve the incalculable and the intractable. The computational and algorithmic turn in security has no tolerance for the emergent or half-seen figure at the edges of perception, no interest in an unfulfilled future potential. 'All possible links' are wrought in the correlative relations that are drawn between bodies as they are disaggregated into degrees of risk. There is a challenge for law and human rights when a juridical sensibility of evidence and evaluation meets a set of security measures that demand the projection of future possible events yet to take place. Where the balance of probability may discount unverified fragments, computation lends greater weight to the associated elements, such that once assembled together their singular uncertainty it less easy to see.

So, *is privacy as a body of rights adequate to the task of protecting the capacity to make a political claim?* If the politics of privacy is to locate space to challenge the analysis of 'big data' (Boyd and Crawford 2013), then, one step may be to make a

distinction between privacy as a body of rights and privacy as a claim that can be made. The body of rights, as Costas Douzinas (2000; 2012) reminds us compellingly, embodies an imaginary unity of the self, a clearly identifiable subject, while the rights claimant is fractured and split. Whilst the right to privacy itself is readily reconciled within the technology – 'anonymising', 'masking', or 'depersonalizing' the data, for example – the fractured subject falls beneath the register of recognisable rights. Yet, where the body of privacy rights is inadequate to the task of responding to contemporary forms of security, the claim to privacy can be a political claim made by those whose experiences and lives are not registered in a body of rights.

## References


Boyd, Danah and Kate Crawford (2013) 'Critical questions for big data', *Information, Communication and Society* 15: 5.

de Goede, Marieke (2012) *Speculative Security: The Politics of Pursuing Terrorist Monies*, University of Minnesota Press.

Deleuze, Gilles (1992) 'Postscript on the societies of control' *October* 59: 3-7.

Douzinas, Costas (2000) *The End of Human Rights: Critical Legal Thought at the Fin-de-Siecle*, Oxford: Hart.

Douzinas, Costas (2012) 'The paradoxes of human rights', *Constellations* 19: 2.

Keenan, Thomas (1997) *Fables of Responsibility: Aberrations and Predicaments in Ethics and Politics*, Stanford University Press.

Mayer-Schönberger, Viktor (2009) *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press.

Obama, Barack (2013) 'Remarks at Whitehouse press conference, August 9 2013', available at http://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference