Science as Culture, 2016
http://dx.doi.org/10.1080/09505431.2016.1255723

Security Technologies Versus Citizen Roles?

GOVERT VALKENBURG

Department of Technology and Society Studies, Maastricht University, Maastricht, The Netherlands

ABSTRACT *The idea of securitization holds that perceived threats and the ensuing need for security measures are mobilized in speech acts to legitimate bypassing of normal practices of democratic politics and justification. Citizens, as members of the political community, are thus effectively deprived of their agency. Attempts at securitization gain clout from the severity of the mobilized threat: the more convincingly a threat is argued to cause disruptions in the functioning of society and ultimately the loss of human life, the more acceptable it will become to bypass democratic governance in order to prevent the threat. Accordingly, security technologies can be conceived of as those technologies that are constructed and mobilized in such attempts at securitization and depoliticization. However, security technologies can also be thought of as technologies that are mobilized in face of existential threats more generally, regardless of whether their mobilization has a depoliticizing effect or not. Yet, as case studies on airport security scanners and security in smart grids show, not all implementations of security, even against existential threats, show this tendency of depoliticization as essential in securitization and in technologies of security. This article further demonstrates that the agency of citizens in the governance of these technologies importantly depends on whether or not the threat is perceived as internal or external to the referent object of the security programme.*

KEY WORDS: securitization, citizenship, security technologies, airport security, smart grids

Introduction

On 7 June 2013, President Obama argued that intensive monitoring of US citizens' phone and Internet activity is justified in view of imminent terrorist threats. In the

Correspondence Address: Govert Valkenburg, Department of Technology and Society Studies, Maastricht University, Maastricht, The Netherlands. Email: g.valkenburg@maastrichtuniversity.nl

press, the programme was primarily discussed in terms of the privacy encroachment it posed. While some safeguards were being put in place, such as the monitoring of the surveillance practices by judges and the approval of the plan by Congress, these were insufficient to take away these concerns. Importantly, White House officials were summoned for further public account of why such an encroachment was needed in the first place (Spetalnick and Holland, 2013).

What we see here is an attempt at securitization, or a speech act by which something is declared to be the subject of a security regime. This act serves to exempt that issue from normal political and social standards (Buzan *et al.*, 1998). The vocabulary of security, if used in a political context, has the potential for suspending fundamental principles that are otherwise central both to how societies are organized, and to how this organization of society is a matter of politics. For example, an appeal to security potentially sets aside the principle of democratic account. And it potentially outweighs basic rights, such as the right to privacy and the right to freedom of movement.

At this point, I am interested in exploring how and where this depoliticization, if successful, is accomplished in practice. Exempting something from politics requires keeping control over agendas, silencing particular voices, and preventing specific harms from becoming visible and raising a concern. This merits explanation beyond merely stating that politics is silenced, and requires engaging with the question of where and how such construction of non-politics takes place. Only after this is made visible, does it become possible to duly assess whether or not depoliticization is an inevitable consequence of constructing security.

Second, I will investigate how such construction of security takes place through the arrangement of technologies. There might be something particularly depoliticizing to security technology; if not in any essentialist way, then at least in a practical, empirical way. After all, since building security technologies is one of the primary modes of operation when increasing security, if there is anything depoliticizing to security, it might be found in its technologies.

Finally, the third question I am interested in is how the citizen, as the prime bearer of political agency, is positioned. With a particular security regime comes a particular positioning of political institutions and actors, and the citizen is one of these. In the case of monitoring of phone and internet activity, it has indeed been argued that civil-society actors are among the first ones to experience curtailment of freedoms as a consequence of such monitoring (Citizen Lab and Anderson, 2015). More generally, specific kinds of citizens and civil-society practices are co-constructed in acts of securitization. It is likely that such monitoring practices could render certain instances of liaising illegitimate. This would result in people feeling less free to act, the practice may de facto preventing civil society from flourishing.

In accordance with the general idea of securitization, a thought that is often uncritically repeated is that when security technologies are put in place, no room is left for any genuine kind of engagement, political agency or indeed citizenship (see e.g. Zureik and Hindle, 2004; Eubanks, 2006; Schomberg, 2011). Equally, some empirical diagnoses seem to be couched in a vocabulary that renders the two incompatible, by stating that citizens are outside any debate once security technologies are to be implemented (see e.g. Vedder *et al.*, 2007). In a more institutional vein, it has been posited as a general observation that the authority over security practices and security technologies is firmly in the hands of a small professional elite. Thus, not only is the issue itself rendered inaccessible for contestation and politicization, also no critique can be levelled against the politics that steers clear of accommodating such contestation (Monahan, 2006, p. 7).

However, neither conceptually nor empirically is it self-evident that installation of security measures entails such impediments to democratic principles. Even though these impediments are clearly at the core of the aforementioned idea of securitization, one question I still deem critical is whether constructions of security necessarily lead to depoliticization, and to what extent they indeed comply with the idea of securitization. In fact, forms of political engagement and the realization of some sort of security appear together at times. Notably security in smart grids, to be discussed as one of the cases below, shows that the value of security does not in any essential way entail a curtailment of the political. Nor does it curtail the citizens' freedom to engage in that political. In fact, sometimes security regimes and political engagement can be constructed as going together productively.

In the following section, I will first discuss the alleged depoliticizing nature of security, how this is thought more specifically to operate in security technologies, and the repercussions this has in principle for the position of citizens. Then, in the subsequent sections I articulate these relations in two empirical cases. In the third section, the case of security scanners at airports is discussed. Here, threats are constructed as situated in a particular way *internal* to the population that is also to be protected. In the fourth section, the case of security in so-called *smart electricity grids* is discussed. Here, conversely, it becomes clear that threats can also be constructed as *external* to the population that is to be protected. These two cases demonstrate how security and political agency are interdependent in more complex and multiple ways than through a simple trade-off.

Construction of Security

Securitization

The question whether and how the pursuit of security leads to silencing politics connects closely to the notion of *securitization*. The notion is paradoxical, for on the on hand it offers an important conceptualization of how construction of security leads to silencing of politics, while on the other hand it is itself an articulation of the politics of a specific idea of security getting prioritized. The idea of securitization disavows the assumption of an objectively existing existential threat that would inform and justify particular political choices.

The concept was originally conceived of as a speech act in which at once a political community, a threat to a valued referent object, and a legitimated approach to containing that threat are constructed (Buzan and Waever, 2003, p. 491; Stritzel, 2007). 'A successful securitization [...] has three components (or steps): existential threats, emergency action, and effects on interunit relations by breaking free of rules' (Buzan *et al*., 1998, p. 26).

At the same time, the notion of securitization itself suggests an implication of security practices into displacement of politics. Normal politics is trumped by a reference to threats, and replaced by non-normal forms of politics:

> Securitization entails the removal of an issue from the realm of 'normal' (that is,) politics, and into the realm of the exception, of sovereign prerogative. Action toward a security issue may entail the suspension of normal rules, or even an authoritarian approach that eschews deliberation or democratic participation. (Mulligan, 2011, pp. 638–639; see also Williams, 2003)

Remarkably, Salter (2008a) argues that depoliticization, as part of the act of securitization, will be especially successful insofar as it happens by quantification of threats, as well as when protection against those threats is technologically mediated. 'The description of threats to aviation security in quantitative terms, especially when spoken by the expert panel, hides the expansion of the ambit of security in the policing, surveillance, and control of mobile populations' (Salter, 2008a, p. 262). A question I will seek to answer empirically is how this ambit of security is shaped more precisely, and in the next subsection I will offer a distinctly technological perspective on this.

In this light, the close connection between privacy and security brings an additional dimension to securitization. Often, the construction of security technologies is couched in a vocabulary of privacy-sensitivity and accompanied with technical measures to avoid impediments to privacy. However, it has been suggested by Van der Ploeg (2005) in a more general sense, that such approaches, for example, *privacy by design* (Cavoukian, 2009), while solving potential problems along technical lines, by corollary eliminate sites for socio-political interaction. Importantly, a site for building trust is lost. Thus, ironically, a concern for a political right such as privacy can in the end contribute to depoliticization and securitization.

Following this paradoxical nature of the phenomenon of securitization, I wonder how the ensemble of threats, human subjects, political agency, and security are constructed together. How are versions of security built on different notions of threat, and how do these connect to different conceptions of the political, the public, and citizenship? Or alternatively—in line with the idea of *intra-action* (Barad, 2007) that captures the idea that entities constitute one another first in their interaction—how do versions of citizenship, ideas of security, and sociotechnical security settings mutually constitute each other? In the empirical analysis below, it will appear that the freedoms curtailed in pursuit of security are manifold, and not necessarily the same as the ones needed to develop political action—though they can be so in specific situations.

Security Technologies

In practice, the question of what kind of threat and ensuing security regime are to be constructed is not answered only in an orderly political debate. Both threats and security measures are additionally implemented in the technological realm (Aradau, 2010; Valkenburg and Van der Ploeg, 2015):

> The securitization of critical infrastructure reconfigures materialities in the world and creates new hierarchies and forms of exclusion. Interconnectivities and interdependencies do not exist independent of particular materialities—the material-discursive practices that securitize connectivity and dependency exclude materialities of the production of objects, for example. At the same time, these materializations of objects to be protected also intra-act with materialities of economic and geopolitical structures. (Aradau, 2010, p. 509)

In order to get a clearer view of how politicization and depoliticization work in specific cases, we must pay attention to how in those cases connections are made to particular political and material realities.

Material implementation in security devices is not just the implementation of an unequivocally defined notion of security, or a protection against an objectively existing threat. Rather, construction of security technologies is to be seen as fundamentally entwined and even coincident with the process in which security is constructed, along with the construction and mobilization of threats, and a construction and positioning of the citizen. Following Barad (2007, p. 33), I heuristically assume here that ‘distinct agencies do not precede, but rather emerge through, their intra-action’. There is no such thing as a prior citizen, prior security, or a prior ideal security technology; let alone a security that is unequivocally implemented into technology. Rather, there are the connections between them that make them emerge, and security technologies are themselves important actors in this process of mutual constitution.

Even within a constructivist perspective on security technologies, there seems to have been a gradual and consistent change over the past decades in how security technologies operate. From a traditional means-ends rationality, they have moved towards a risk-management rationality:

> From this viewpoint, a safer society is often pursued through the implementation of security policies that increasingly rely on the deployment of

> [Surveillance Oriented Security Technologies] and interconnected data exchange systems in order to transform unknown threats into predictable events. (Pavone and Esposti, 2012, p. 557)

This change seems to be accompanied by the apparent presumption that such technological implementation potentially compromises political rights, witness a statement of (then) EU Vice-President Franco Frattini quoted in the same text: ‘Our goal remains preserving the right balance between fundamental right to security of citizens, the right to life and the other fundamental rights of individuals, including privacy and procedural rights’ (Pavone and Esposti, 2012, p. 558 referencing Frattini from a 2007 press release).

If we understand securitization as a distinct version of politics—namely a politics of depoliticization—then we should attend to the question how this version of politics fits in with the slogan of technology being ‘politics by other means’ (Latour, 1988). One distinctive aspect of technology is its ability to become (or be made into) a black box, or an entity of which the genesis and the politics controlling this genesis becomes invisible (Latour, 1987). The politics fades from view because the actors doing the politics have no need to remain on stage once the technologies are fixed in place. In fact, it is at the heart of construction work that the work done is also attempted to be made invisible. Efforts are continually made to obfuscate the lines of connection between underlying struggles and the emerging sociotechnical configuration (Latour, 1993, 2010). The more actors succeed in concealing the work going into the construction of sociotechnical configurations, the more these sociotechnical configurations appear as factually self-evident, morally just, or simply given.

Positioning the Citizen

Whether along technological lines or in a more generic sense, politicization and depoliticization are about positioning political actors in particular powerful or disempowered ways. This is not least about positioning the citizen. It is not self-evident how a citizen, as a member of a political community, is granted political agency. Especially in the case where normal politics is bypassed, disempowerment of the citizens is likely to be the case.

Clearly, as in any process of construction, the emerging ensemble of technological and social structures serves less the interests of parties who were not included in the design process. Security technologies show a potential reflexivity in this respect: if people themselves are the bearers of threats against which security is to be organized, it is likely that their political agency will be curtailed. Consequently, their opportunities to contest the specific construction of security are diminished, including the construction of themselves as threats in the first place.

Walters (2014) shows how the construction of drones and drone warfare explicitly serves the political displacement of certain actors, hence limiting access to politics in specific ways. Such displacement will be more successful if the technologies involved are constructed in such a way that the political negotiation of the justifying threats are more successfully made invisible. This goes together well with the depoliticizing tendency in securitization practices and the preference to keep things secret; things that are not a discourse in the conventional meaning are easier to keep off the political agenda:

> But, what happens in situations where the controversial things in question are simply not readily available or accessible to the public? What pattern do controversies follow when the things in question are secreted away, or only very partially disclosed? What happens when the material things in question are absent presences? What happens when making certain truths public carries the risk of death [. . .]? Such questions are made pressing when we are dealing with issues of national and international security, with domains falling under the title of foreign policy, where laws and cultures of secrecy are operative and covert activity widespread. (p. 112)

In similar vein, in the case studies below, I will investigate whether and how the underlying security concerns are closed down and rigidly inscribed into technology, or conversely implemented in a more open way that leaves some flexibility to interpretation. Security concerns are mobilized as a legitimation for technological and institutional solutions which then appear as inevitable, and immune for political scrutiny:

> [S]ecuritization reflects the complex constitution of social and political communities and may be successful and unsuccessful to different degrees in different settings within the same issue area and across issues. [. . .] [S]tudies of securitization need to account for the movement of issues into and out of the security sector over time. (Salter, 2008b, p. 324)

But studying securitization is about more than only moving things in and out of security regimes. As Martin argues regarding the constitution of the subject in airport security regimes, '[. . .] the informationalization of language and the objectification of the body as a representation of pre-thought intentionally *displaces* the traditional, liberal subject as the center of security regimes' (2010, p. 30, emphasis original).

Rearranging actor positions is thus as a central element of securitization. My earlier question was whether every instance of constructing security is also an instance of securitization in that it bypasses normal politics. The above thoughts on the relation between securitization and the construction of security technologies allow for a further specification of this question. If constructing security comes with a rearrangement of political actors, and if part of this construction takes place through technological configurations, then what kind of positioning of political actors is enacted by the technologies that obtain in the end?

Case Selection and Method

From the above review, I arrive at three questions that are to be answered empirically. First, it needs answering for a particular case whether and how the mobilization of threats can be seen as an attempt at securitization. Second, I will pay attention to the question how this relates precisely to the particularities of the technologies around which security practices emerge. And third, I am interested in knowing how actors, including citizens, technologies, and threats, are co-constituted, and how citizens emerge as politically empowered or disempowered. In the following, airport security and the security regimes of *smart grids* are studied in the light of these questions.

The reason to select these two cases is chiefly in the observation that one has a clearly depoliticizing effect, whereas the other does not. That is to say, on the one hand, airport security is clearly an instance of securitization in the narrow sense that security and depoliticization go hand-in-hand. On the other hand, in smart grids, even though security is levelled against threats that are vital and serious, such depoliticization is not clearly visible. Thus, whether or not security equals securitization seems to differ between these cases.

One of the defining aspects of securitization is the repositioning of actors. In both cases, the emerging positioning of citizens is most telling of the extent of depoliticization. As in both cases technologies are the most tangible and rigid executors of the security regime, it will be at technologically mediated constructions of citizens where the extent of depoliticization becomes most clearly visible. A further understanding of those technologies is sought by explaining the notion of security that informs the implementation of those technologies.

The two cases were studied through document analysis of both academic and generally accessible (mostly online) sources, complemented with nine semi-structured interviews. The interviewees mostly held an expert position in either the development or the analysis of systems. One of them (in the case of airport security scanners) represented a particular user perspective. The interviews were not explicitly couched in terms of (de)politicization or positioning of citizens, but in more generic terms such as how citizens were supposed to interact with the technologies, how design choices are made on the basis of particular conceptions of, threat, security, and privacy, and how technologies in their operation do or do not live up to expectations. Stylized transcripts were made, and interpreted by the principle of charity (Blackburn, 1994, p. 62), that is, assuming that as much as possible of what the interviewee says is truthful and rational before levelling any critique. Thus, it is prevented that a straw man be set up. All interviews took place between August 2012 and January 2013.

The relevance of interviewing these experts is in their involvement in the actual construction of citizens. As they are dominant in the construction of these security technologies, it is most likely that their interests will be best reflected and served by those technologies. At this point I am not interested *per se* in how successful their depoliticization programmes are, nor in studying which groups are *de facto* excluded from politics. Neither has it been a research concern how things would have been different if currently underrepresented groups had been more influential. Rather, I am interested in the degree of depoliticization as such that is present in the broader programmes of constructing a security regime. Following these experts means following the ones who are doing the actual depoliticization.

Body Scanners: Seeking the Enemy Within

A Privacy-Friendly Security Technology

The first case to be discussed here concerns *active millimetre-wave scanners* (AMS), a novel class of security scanners used in airport security. This type of scanner is capable of detecting items carried on the body that arguably pose hazards to aviation security. In addition to guns and other metal objects that have for long been possible to detect with conventional metal detectors, the new scanner is capable of detecting items made of other materials, including plastics and liquids. Both a security manager at Schiphol Airport and a national security manager I interviewed argue that in addition to a benefit for airport security, this particular type also promises a reduction of turnaround, a reduction of human resources needed—since a larger part of the security assessment is automated—and an increased sense of privacy (see also Schiphol, 2013).

An additional promise is in the fact that the automatic object detection, unlike inspection by a human officer, is not susceptible to the fatigue that humans experience during control-room work, sometimes after only 15 minutes of work. As the national security manager argues:

> During an exam, people perform well. They are focused. But the next day, they are in an argument with their partner, and they keep pondering about that. You see then that they do not do their work properly anymore. This is one of our drives: we want to implement automated detection, because that is better. And our perk is privacy. We had that well in place already, but now it is nearing perfection.

The AMS differs from other body-scanning technologies, including various x-ray scanners that have been in use more widely. Unlike other scanners, the AMS does not produce a picture of the body in any photographic or otherwise visually realistic or recognizable way. Neither does it produce any other representation from which a human observer could recognize or identify the person, or identify particular properties of the body. This differs from photo-realist pictures made by other imaging techniques like x-ray pass-through scanners, x-ray backscatter scanners, or infrared scanners. Instead of a photo-realist picture, a mannequin is shown without any anatomical detail, not even gender. The mannequin always looks the same, regardless of the particular body that goes into the scanner. On this mannequin, only those body parts are highlighted on which suspect materials are found. Subject to the specifications of the security policy, this body part is then to be searched manually by a security officer. This whole socio-technical ensemble, consisting of a mannequin-producing scanner with a partial body search conducted by a human security officer, is considered a smaller privacy encroachment than the full body search ('pat-down') by the same officer. With conventional metal detectors, such searches are often needed on top of the scanning.

The working of the AMS is based on the use of electromagnetic waves in the millimetre spectrum (70–80 GHz). Electromagnetic radiation is emitted to illuminate the body of the scanned person. The amount emitted is several orders of magnitude smaller than what cell phones emanate in the same spectrum. Upon illumination, the millimetre waves are reflected by the body, clothes, and anything else worn on the body. A vast number of sensors receive the reflected waves and record their amplitude and phase. By means of complex signal processing techniques, the system is able to determine whether anything other than clothing is present on the body, and if so, on which part of the body it is located. As one research and development (R&D) engineer reports:

> We see our task actually to distinguish between something which belongs to normal clothing, and just natural human parts, like hands, and something which is anomalous to this. So, if there is something strange, there is something that needs control. We can of course go a step further, and try to classify the object or to classify the material, and start to give more information about this, but that is a matter of developing algorithms for that, which is not the main purpose of our concept now. Because in many practical cases, when there is something strange, something suspicious, then manual controlling is needed.

Airport Securitization?

At first sight, it seems that this technology, with the practice of operation surrounding it, is the next best thing in airport security: better detection takes place at a smaller privacy encroachment. However, at closer look, this improved form of security is more than just that. In view of the concept of securitization, the question bearing enquiry is whether and how this particular form of security may or may not lead to trumping normal politics and replacing it by some form of emergency politics. Even if airports are not exactly sites of politics in the same way parliaments and op-ed pages are, in this case it remains a valid question to ask whether installing a security regime leads to a situation that resembles non-normal politics, or in a broader sense the lifting of basic civil rights. It is pertinent to see whether demands for justification are put aside, whether appeal and voicing of concerns are still possible, and in general what kind of agency is allotted to the general audience.

To articulate attempts at securitization in the case of airport security scanners, it is revealing to zoom in more closely on the threats that are mobilized to inform and justify the security practice. It turns out that a more complex ensemble of threats is mobilized than simply terrorism. Also, we see that how these threats are de facto consolidated in the sociotechnical practice of the security scanner and human officers, prioritizes specific threats as relevant. As I will further explain, the threats against which security is organized are narrowed down to very specific technical conditions: of when a human body is vetted as normal, and when it is classified as suspect. Also, following a heuristics based on Barad's (2007) notion of intra-action, this is not only a matter of construction in political, discursive terms, but also of a confrontation with the technological possibilities available at the time of development.

By means of an example, I will show how a problem of this kind occurs around people with a stoma (artificial colon exit). As scanners are now able to detect other materials than metals, the medical devices that people have to carry to manage their stoma are suddenly made relevant to the security practice. In fact, the system enacts stoma patients as belonging to the same class as people with terrorist motivations. As one spokesman of an interest group for stoma patients reports, 'people were summoned to show what is hidden under their clothes, just on the spot. That is of course utterly unacceptable, and it is in some cases even quite difficult. It isn't always technically possible to just show it, and you need a lot of water as well'.

The security practice at first seems to do no more than conducting a technical operation. The practice operates on all air travellers, which it then divides into a suspect fraction and a non-suspect fraction. However, the two actor perspectives above illustrate how this becomes a conflictual matter; what is an anomaly for one, is a very private and bodily affair for the other.

While the misclassification is a great inconvenience for all whom it concerns, it is only a small problem when viewed as a percentage of the whole population of air travellers. This means that, if democratic principles of protecting minority rights were not in place, the practice would probably continue, allowing the problem to persist. This is pressed further by the claimed need to process the entire population without exceptions, as the following account of the spokesman of the patients' interest group shows: '[Security operators] were weary of discussing the matter with us [the stoma patient interest group, GV]. Only after we had stipulated that we would not plead for an exemption from security procedures, they showed willingness to address the issue.' In other words, it is discursively enacted that stoma patients are just as suspect as any other member of society, which means that the suspicion cast on the whole population and the absence of possibilities for appeal are fixed in place. While this part of the construction of stoma patients as suspect happens through discursive acts, and while it is a brief moment of politicization, this is immediately followed by a depoliticization which is chiefly traced back to how this specific AMS technology works and operates.

What is more, the problem of misclassification of stoma patients shows that the protected population and the suspected population coincide, if we look solely at the technological performance of the system. At face value, underlying ideas of threats seem to consist mainly of items that are not to be brought on board air planes: bombs, weapons, and drugs. However, in the interaction between the scanners and the airport travellers, a much broader and less articulate set of questionable threats emerges, including things that would not be reckoned dangerous in any meaningful sense of the word, such as stomas. First, this entails that stoma issues inherit from their classification as threat a high degree of depoliticization. Second, this depoliticization of stoma issues is also to some extent *required* for the security practice to operate and keep in place the working definition of threat. This specific version of threat has become immune to further contestation by its materialization into this particular AMS class of scanners (Valkenburg and Van der Ploeg, 2015). And third, on top of the fact that body scanners in general already enact just any traveller as suspect, the specific technological implementation renders some members of the innocent population even more suspect than others.

While actual numbers of intercepted guns and bombs as well as false positives are kept secret, it is confirmed by both the Schiphol security manager and the patients' representative that the problem of medical devices and prostheses triggering alarms is substantial. Thus, the system design actually translates an initial idea of threat into a technology-mediated classification of nonstandard bodies. The boundary between trusted and mistrusted bodies is fuzzy, and it is not evident that the line is drawn at wearing a gun. What is more, instances of misclassification are false from the perspectives of the misclassified traveller and the security operator, but not from the perspective of design specifications of the AMS. Even though false alarms are usually resolved in the end through fallback routines executed by human actors, it does perpetually confront the benevolent fraction of the population with the fact that malevolent actors are present among them. The threat against which securitization is offered, emerges as part of the population itself.

The materiality of the AMS renders the definition of threats in an obdurate way. Regardless of the intentions and specifications with which the AMS was designed, it *de facto* tells us what a threat looks like and leaves no further room for contestation. The most important threat about which knowledge is available in that particular situation is the threat identified by the AMS. Consequently, the freedom of the person to act is limited. As the threat coincides with the person, containment of the threat means containment of the person. This leaves little room for any kind of engaged citizen to emerge.

In fact, the internalization of threat is not limited to the level of social action. It intrudes even into the body, as a specific enactment of threat by the technological implementation of security. Ironically, one of the primary claims in legitimating the AMS is in its arguable non-invasiveness and its inability to intrude into the body. As the R&D engineer reports:

> We are not able to look inside the body. We stop at the skin. [. . .] So we see our task actually like to distinguish between something which belongs to normal clothing, and just natural human parts, like hands, and something which is anomalous to this. So, if there is something strange, there is something that needs control.

The sting is in the tail. It is in this overflow of additional control that the boundaries of the body are challenged and renegotiated, and in a way that renders stoma patients the subordinate party.

Depoliticization entrenches the airport and its security in additional ways. First, the implementation of the AMS seems to comply well with the aforementioned ideas of *privacy by design* (Cavoukian, 2009), that is, the ideology that technologies, also security technologies, are to be arranged in such a way that they promote rather than threaten privacy. Indeed, a scanner that does not make any nude pictures, let alone present or store those pictures, is arguably more respecting of privacy than a scanner that does. However, as noted earlier, this also means the elimination of yet another issue that could serve as a site for politics, as a means to unite a public, or as an object for the public to engage with. Moreover, this mechanism can be extended here: not only is a site for politics eliminated, also the definition of the political itself is *de facto* made into a black box, as it is the technology that presents the final definition of threat. This then also defines the boundaries of (normal) politics.

In much the same way, positioning the AMS as a safe device works (at least *de facto*) as a means to depoliticize it. Indeed, in the case of AMSs, passenger safety is argued to be safeguarded in multiple ways. The radiation is, according to scientific consensus, completely harmless. It cannot pass through the body, nor does it have any effect on the body. It is of similar wavelength as the radiation we continually experience from mobile phones or car radars, be it at immensely lower intensity. Hence, even if we were mistaken in the harmlessness of the radiation, the AMS would still be the last problem in line, far below car radars and mobile phones. If a technology can be presented as absolutely safe, the whole matter seems to be easier to expel from the political realm.

In this particular form, the enactment of threat has a largely depoliticizing effect. Because of the coincidence of the threat and the population that is to be securitized, the latter could not logically be granted political agency. While airport security is not in any obvious way a typical site for (direct) democratization, the observation that airport security works in a depoliticizing way is a bit more than a truism. Indeed, looking at the procedures and the interaction between the AMS and citizens, it appears that the whole practice of airport security is geared towards eliminating the passenger as a present person, and making the passenger into something manageable because personal aspects are made absent (Bellanova and González Fuster, 2013).

The version of security that emerges in airport security practices and technologies, and the ensuing positioning of actors, is one in which the protected community coincides with the threatening community: terrorists are sought within the population of protected traveller-citizens. This has two consequences. First, it shows that even if political agency for citizens is not necessarily at odds with security, it appears at least that *this* security works in that depoliticizing direction. Second, even if airports are not considered institutions that need democratization in a direct sense, this particular version of security pre-empts any attempt of engaging with airports.

Smart Electricity Grids: Engagement and External Threats

The Future of Electricity Provision

Smart electricity grids spell the future of electrical power networks. They replace the conventional electricity infrastructure that consists of centralized power plants that deliver electrical energy in one direction to end consumers. Instead, smart grids are to perform a much broader range of functions in the accommodation of electrical energy. Smart grids are considered smart because they intensively use information of various sorts. This smartness is considered necessary for the accommodation of novel, renewable energy sources, as well as for further improvement of the security of energy supply and the efficiency of energy use.

One important operational function on which smart grids differ from conventional grids, is that power infrastructure becomes capable of transporting electrical energy in multiple directions. A terminal is no longer essentially a source or a drain of energy, but may alternate between these two functions. This is a vital functionality in a world where individual users may at one moment consume electrical energy from the grid, and at another moment deliver energy to the grid. This happens for example when their photovoltaic cells produce more energy than their household can use. Another novel function is the active balancing of production and consumption of energy at a specific moment. For example, energy-intensive tasks such as water heating, running a washing machine cycle or charging an electric vehicle can be performed when there is a surplus of—hence cheap—electrical energy. Market mechanisms can be installed to strike this balance.

The smart grid is an important means to facilitate the transition towards the use of low-carbon energy sources. The deployment of intermittent and distributed sources such as wind turbines and photovoltaic installations requires the multi-directional transport and matched consumption that smart grids can facilitate. The availability of these energy sources is only predictable to a limited extent, which puts additional demands on the storage, distribution, and consumption of energy. Also, as one security specialist at a distribution system operator (DSO) explains,

> We see a lot of developments happening. Sustainable energy, maybe electric vehicles somewhere soon. The future is uncertain, but we have to be ready for it. You can do that with more copper[1] and to some extent with power electronics, but more is to be done. [. . .] With copper, it would take billions to bring the network up to par. With intelligent technology, you can do this a whole lot cheaper.

At a strategic level, the smart grid is staged as an important means of combating geopolitical and ecologic hazards. Its flexibility reduces the dependency on all too specific energy resources. In addition to the aforementioned incorporation of novel, renewable energy sources, this reduces the dependency on coal and oil suppliers. As the latter are de facto importantly based in politically unstable regions, smart grids are believed to contribute to energy security. Thus, smart grids are themselves security technologies of some sort. I do not engage further with energy security here, but it is part of the background against which the securing of smart grids themselves gains importance.

These novel functions, to be performed by smart grids, depend on communication of data. To this end, a layer of information and communication technologies is added to the layer of power transport—the actual electrical energy still flowing through the same power network of copper and iron, but now managed in a more data-intensive way. With the development of smart grids, the distribution of electrical power becomes increasingly intertwined with the realm of information and information technologies. In a way, the energy grid becomes itself an information infrastructure.

Through this conflation of the energy sphere and the information sphere, the energy network becomes exposed to the same kind of vulnerabilities as do other information infrastructures: various forms of hacking, issues of privacy and data protection, digital forms of fraud, and so on. Ultimately, loss of control starts looming as a new threat. Losing control over the smart grid will disrupt society at large. Social and economic processes will come to a halt, and ultimately lives may be lost. Subversive parties can show off the power to assume control, installing great fear throughout society. Such acts straightforwardly classify as terrorism, and thus we begin to wonder whether accordingly, attempts at securitization and depoliticization should be found.

The fear of losing control seems justified. Cyber-attacks have already been reported on power facilities causing power blackouts in Brazil (CBS, 2009; Allan *et al*., 2010), even though the account of the blackout being the result of a cyber-attack has been questioned (Harris, 2009; Krebs, 2010; WikiLeaks, 2011). Also, security breaches in US utility networks by Russian and Chinese spies have been reported (Gorman, 2009), and in Germany still as recently as 2012 (EurActiv, 2012). Accordingly, the electrical power infrastructure is classified as a so-called critical infrastructure (European Commission, 2004, p. 3; Burgess, 2007, p. 475; Hämmerli and Renda, 2010), which is to say that it is to be of primary concern in security assessment. It is worth noting, though, that the mentioned events have not had a game-changing impact like 9/11 had for airport security.

One potential mechanism underlying the loss of control is substantiated by a researcher I interviewed at a scientific consulting firm. The point of connection between a household and the smart grid is identified at the *smart meter*. This device measures energy consumption in a detailed way, and makes the measurement data available to both the user and the utility service. The smart meters available at the time of interviewing, early 2013, have a built-in possibility for remote switching. This enables power suppliers to switch off a specific connection, for example a household that repeatedly fails to pay its due balances.

First, this has questionable consequences for households, especially in view of the possibility that the household's payment history is stored incorrectly. Second, a novel exposure emerges at the system level. If cybercriminals manage to gain control over a vast number of these meters, they can switch them all off at the same time. This entails that the power demand will instantly drop. As power plants cannot be switched off accordingly rapidly, a power surplus will rapidly accumulate in the system. This will lead to various sorts of meltdowns, taking vast parts of the system offline for several months. As one information architect at a DSO points out, similar disruptions could be caused by large-scale forgery of sensor data.

At the time of interviewing, a directive had been issued that prohibited the utility services from being used by the switching facility. However, this is questionable as a security measure, since it disregards the material reality of the meter. As the switching functionality is technically still there, the meter *de facto* keeps exposing the vulnerability. At the same time, this makes clear that warranting individual autonomy and agency requires largely the same protection as does the safety of the system. What is needed is a proper degree of access control to the meter.

Smart Grid Citizens?

The various security aspects discussed shed new light on the question how actors are repositioned. Does the consumer emerge as something resembling a citizen?

And does this incur a replacement of normal politics by some non-normal form of politics? It seems to require little further argument that the geopolitical issues of energy security have little or no consequences on how the citizen are positioned vis-à-vis the smart grid. No connection of this kind occurred during the interviews, nor did it in the other sources. Still the observation is relevant. It signifies that this conception of security does not entail a connection between the consumer and the threat. This precludes the need to depoliticize the consumer and the need for securitization in the strict sense defined above.

Things are potentially different in the other two security perspectives: the loss of control at the network level and the violation of individuals' privacy. At least principally, the individual person could be a suspect when it comes to hacking the smart grid, and when it comes to misusing privacy-sensitive data generated by the smart grid. What kind of security regime is constructed here, and what position for the individual person obtains? In face of both threats, security is chiefly shaped as cyber security, to which the following analysis will indeed be limited. (Of course there is also a practice of physically securing important network nodes, but this is not interesting from a securitization perspective, as these are not places that are natural for the general public to enter, nor to which limiting the general public's access is politically exceptional.)

In this cyber sphere, security is primarily shaped as principles such as data minimization, segmentation and separation of information flows, separation of roles between suppliers of different services, and so on (Rial and Danezis, 2011; Cavoukian and Dix, 2012). The aforementioned information architect explains how in a process of energy delivery, different actors such as the energy producer, the distributor, the provider of a particular energy service at a specific point, and so on, each only avail of the information they exactly need to provide their part of the service. In other words, the stuff on which perpetrators could possibly operate, is deliberately dispersed and disconnected. In view of the previous case and the very concept of securitization, this is already a remarkable way of doing security politics. Security is not produced by ensuring a firmer grip on people and affairs, but by arranging technological configurations in such a way that perpetrators cannot get a grip on them.

In this construction of cyber security, the consumer is largely left untouched. The consumer is not treated as a suspect, and it is hard to see how the security measures compromise their freedoms. With respect to privacy, the consumer is not bothered that much either; rather, the consumer is protected against privacy threats through the same mechanisms that also protect the system against cybercrime and terrorism. The security measures in smart grids have no tangible consequences for consumers, as far as their freedom to take consequential decisions and to organize their own lives is concerned. They also remain free to choose the ways they manage their energy, or the ways they relate to collective energy affairs.

If no significant repositioning of the consumer emerges, a second question becomes relevant: can any form of non-normal politics be discerned, which would impinge upon the identity of the individual as a citizen? Observing an absence of non-normal politics runs the risk of being found caricatural, if anyway the sphere of smart grids is not considered a place for politics. Yet, with smart grids some forms of politics can be found. But unlike the practice of airports security, this politics is not of a non-normal kind.

One instance of such politics is the appropriation of energy challenges by communities. One interviewee works at a DSO as a researcher on the development of user interfaces for smart meters. She reports that if the need for energy reform is convincingly argued, and if it is sufficiently shown how smart grids and smart meters can offer resilience in face of this vulnerability, many people do endorse smart grids:

> This is partly based on less tangible motivations. It is socially desirable to contribute to these kinds of things. It gives a good feeling and it is aimed at the future. The environment is declining, and energy sources are running out.

Taking such a responsibility is in itself an act of engagement. She continues: ‘Rationally, people are perfectly aware that their choices are influenced. … But if they are asked about their energy savings, they argue that they are better off this way.’ Also, after a process of domestication and adaptation, in which consumers develop a more substantive relation with the meter, it turns out that they do not feel particularly controlled, but rather empowered to manage their own power consumption.

In a way, the smart electricity grid provides a substrate upon which specific publics can emerge. The substrate is not a public sphere in the conventional sense of a site where debates are conducted, but it is a site where people engage in particular ways with common concerns. The smart grid translates the common concern of protecting energy supply, and makes it apt for engagement within the private household (Marres, 2009). Importantly, none of what circulates in this sphere calls for targeting the citizen as a potential perpetrator in the same way as does the AMS in airports, and none calls in any specific way for depoliticization. Actors are at least not positioned in a politically disempowered way. Quite the contrary, this form of security politics mobilizes the citizen for the common good of environmental sustainability and a decreased exposure to geopolitical instability, without explicitly curtailing the freedom of the citizen.

How is it possible for citizens to emerge in this security regime as empowered, rather than curtailed and objectified? In the case of smart grids, the threat is not identified inside the population of people who may have a claim to political access. Thus, there is no need to incapacitate the citizen for him or her to be secured. Even if a game-changing event such as 9/11 had occurred in the sphere of energy grids, it is hard to imagine how this could bring the general audience under a security regime that is harsh in a way comparable to airport security. Even if just any citizen were approached as a potential hacker, it is most likely that they will first notice strict security measures when they actually engage in hacking, though this might change if more intricate interactions with the system become part of what is normal for a citizen to do.

Conclusion

Co-constitution of Threats, Technologies, and Citizens

Through the cases, I have illustrated that the kind of practices that ultimately emerge, largely depend on how particular threats, technologies, and citizen agencies are mobilized, and how they co-constitute one another. The claim that depoliticization is a natural consequence of implementing security in technologies (Salter, 2008a), thus requires further qualification. The cases show that there is no essentially depoliticizing tendency in security technologies, but rather different kinds and degrees of depoliticization in each case.

The cases also help to show that the design of technologies matters to the kind of citizenship that emerges. However, citizenship, political agency and engagement and the like are not *per se* a primary concern in the design of these technologies. Rather, once the technologies are introduced into practices, they start to interact with citizens and thereby coproduce new versions of citizens. Also, I observed that the definition of the citizen is less fixed in the case of smart grids than in airport security. In explaining this, the most important differences seem to be the location and the actors at which the threat is identified. Compared to the terrorist threats against which airport security is arranged, it occurs that the agents imposing the threat to smart grids are situated far more distantly. Consequently, it happens that security measures are not visibly targeted at just any energy consumer—unlike airport security, which basically targets any and all travellers. While all travellers must be thoroughly checked at the airport because one of them might be a terrorist, no invasive security measures are imposed on people in the context of their energy consumption just because one of them might have evil plans.

In addition to the way threats are mobilized, I noticed a difference in how the human subject is positioned as a citizen, a consumer, or a potential terrorist. In the smart grid, the human subject is positioned as a vital part of the system itself. In airport security, conversely, the human is merely an object upon which the system acts. Remarkably, in neither case is citizenship explicitly mobilized for the sake of security. But different underlying conceptions of citizenship can be recognized. In the whole mobilization of smart grids, a citizen emerges who co-owns the issue of sustainable transitions and energy security. In airport security, a citizen emerges who is subject to top-down forms of control, where no form of democratic engagement whatsoever seems possible.

With airport security, this leads to a culmination of material-semiotic structures that defy any enactment of the citizen as an actor or as a potential member of a public. With smart grids, conversely, security is much more naturally merged with other values and moreover arranged in such a way that it does not enact citizens themselves as perpetrators.

Security with Citizenship, Not Securitization

Given the observation that security does not necessarily entail depoliticization, I want to ask whether implementing security can always be done in a non-depoliticizing way. Could it work, perhaps, to simply prioritize different forms of threat? Or would maybe different technologies bring out different, less burdening forms of depoliticization? One could wonder whether the depoliticizing character of airport security could be mended simply by having it informed by a different version of threat.

In practice, revision is difficult because existing versions of security have been consolidated in material and organizational structures that came to being under particular distributions of social power. These distributions have led to the interests of some groups being accounted for and not those of others (Valkenburg and Van der Ploeg, 2015). Additionally, it is not quite the case that threats, technologies, or even the relevant actors can be selected at wish.

Nonetheless, some choice might still be left. It is not given *a priori* how threats are to be mobilized to inform the design of security technologies. As technologies are not empty receptacles for discursive matters, nor fixed sources of meaning (Barad, 2007; Aradau, 2010), input to the co-constitutive process of developing security practices can be selected strategically. As it is not self-evident which actors' interests are to be taken into account when security technologies are devised, taking proper care of the democratic processes in which threats are mobilized could help finding more beneficial arrangements.

The idea of securitization as originally defined includes a move of depoliticization, which is even essential for the definition. The above analysis shows that not all implementations of security have this depoliticizing effect. A trivial argument would be that they are not in fact instances of securitization. However, at the same time the threats against which the non-depoliticizing forms of security are arranged, are of a disruptive potential and comparable to the threats central to securitization studies. Thus, it seems better not to discard the examples as inapt, but to propose revision of the idea of securitization.

What these two cases together make clear is that citizenship and security are not essentially at odds, and that security technologies are not essentially depoliticizing. It is not even the case that security has a depoliticizing effect whenever the threat it counters is of an existential kind. Even in face of existential threats, it is possible for security to be compatible with forms of politics that comply with general principles of democracy, engagement, and human freedom. Rather than security per se, it is the exact kind of threat that is mobilized, how this threat is mediated by the particular security technologies, and the way the threat is enacted as connecting to the relevant community, which determines how and to which extent normal politics will be bypassed.

Acknowledgements

The author is greatly indebted to two anonymous reviewers and the editors of this journal for their substantial comments, as well as to Hans Schouwenburg and Andreas Mitzschke who made a great effort to help this article develop. Thanks to Irma van der Ploeg for the collaboration during the empirical research, and Erik Aarden for co-organizing the session at 4S/EASST, 2012, that provided the cue for developing this argument. And thanks to Annapurna Mamidipudi for substantially improving my English usage.

Disclosure statement

No potential conflict of interest was reported by the author.

Funding

The empirical part of this research was conducted at Zuyd University of Applied Sciences as part of the PRISMS project (www.prismsproject.eu), funded by the European Commission under the 7th Framework Program, within scheme FP7-SEC-2011-1, under [grant number 285399].

Note

[1] Among electrics engineers, ‘copper’ is shorthand for that part of the power network that does the actual energy transport, chiefly the power lines.

ORCiD

Govert Valkenburg http://orcid.org/0000-0001-7045-9878

References

Allan, S., Trapp, E. and Scott, A. D. (2010) *Critical Infrastructure Protection for the Smart Grid* (Los Angeles, CA: Accenture).

Aradau, C. (2010) Security that matters: Critical infrastructure and objects of protection, *Security Dialogue*, 41(5), pp. 491–514.

Barad, K. (2007) *Meeting the Universe Halfway: Quantum Physics and the Entanglement of Mater and Meaning* (Durham, NC and London: Duke University Press).

Bellanova, R. and González Fuster, G. (2013) Politics of disappearance: Scanners and (unobserved) bodies as mediators of security practices, *International Political Sociology*, 7, pp. 188–209.

Blackburn, S. (1994) *The Oxford Dictionary of Philosophy* (Oxford: Oxford University Press).

Burgess, J. P. (2007) Social values and material threat: The European programme for critical infrastructure protection, *International Journal of Critical Infrastructures*, 3(3/4), pp. 471–487.

Buzan, B. and Waever, O. (2003) *Regions and Powers: The Structure of International Security*, Vol. 91 (Cambridge: Cambridge University Press).

Buzan, B., Waever, O. and De Wilde, J. (1998) *Security. A New Framework for Analysis* (Boulder, CO: Lynne Rienner Publishers).

Cavoukian, A. (2009) *Privacy by Design: The 7 Foundational Principles* (Toronto, ON: Information and Privacy Commissioner of Ontario).

Cavoukian, A. and Dix, A. (2012) *Smart Meters in Europe, Privacy by Design at its Best* (Toronto, ON: Information and Privacy Commissioner of Ontario).

CBS. (2009) Cyber War: Sabotaging the System, *60 minutes*, November 6.

Citizen Lab and Anderson, C. (2015) *The Need for Democratization of Digital Security Solutions to Ensure the Right to Freedom of Expression* (Toronto: Munk School of Global Affairs).

Eubanks, V. (2006) Technologies of citizenship: Surveillance and political learning in the welfare system, in: T. Monahan (Ed.) *Surveillance and Security: Technological Politics and Power in Everyday Life*, pp. 89–108 (New York and London: Routledge).

EurActiv (2012) *European renewable power grid rocked by cyber-attack.* December 12. Available at http://www.euractiv.com/energy/european-renewable-power-grid-ro-news-516541 (accessed 14 December 2012).

European Commission (2004). *Critical Infrastructure Protection in the fight against terrorism*, Vol. 702 (Brussels: European Commission).

Gorman, S. (2009) Electricity grid in U.S. penetrated by spies, *The Wall Street Journal*, April 8.

Hämmerli, B. and Renda, A. (2010) *Protecting Critical Infrastructure in the EU* (Brussels: Centre for European Policy Studies).

Harris, S. (2009) Brazil to ‘60 minutes’: It wasn’t a hacker. *The Atlantic*, November 10.

Krebs, B. (2010) Cable: No cyber attack in Brazilian ’09 blackout. *KrebsOnline*, December 3.

Latour, B. (1987) *Science in Action: How to Follow Scientists and Engineers Through Society* (Cambridge, MA: Harvard University Press).

Latour, B. (1988) How to write the prince for machines as well as for machinations, in: B. Elliott (Ed.) *Technology and Social Change*, pp. 20–43 (Edinburgh: Edinburgh University Press).

Latour, B. (1993) *La clef de Berlin et autres leçons d’un amateur de sciences* (Paris: Éditions la Découverte).

Latour, B. (2010) *On the Modern Cult of the Factish Gods* (Durham and London: Duke University Press).

Marres, N. (2009) Testing powers of engagement, *European Journal of Social Theory*, 12(1), pp. 117–133.

Martin, L. L. (2010) Bombs, bodies, and biopolitics: Securitizing the subject at the airport security checkpoint, *Social & Cultural Geography*, 11(1), pp. 17–34.

Monahan, T. (2006) Questioning surveillance and security, in: T. Monahan (Ed.) *Surveillance and Security: Technological Politics and Power in Everyday Life*, pp. 1–23 (New York and London: Routledge).

Mulligan, S. (2011) Energy and human ecology: A critical security approach, *Environmental Politics*, 20(5), pp. 633–649.

Pavone, V. and Esposti, S. D. (2012) Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security, *Public Understanding of Science*, 21(5), pp. 556–572.

Rial, A. and Danezis, G. (2011) Privacy-preserving Smart Metering. Paper presented at the Workshop on Privacy in the Electronic Society 2011, Chicago, IL, October.

Salter, M. B. (2008a) Imagining numbers: Risk, quantification, and aviation security, *Security Dialogue*, 39(2–3), pp. 243–266.

Salter, M. B. (2008b) Securitization and desecuritization: A dramaturgical analysis of the Canadian air transport security authority, *Journal of International Relations and Development*, 11(4), pp. 321–349.

Schiphol (2013) Airport security: Security scan. June 21, 2012. Available at http://www.schiphol.nl/web/file?uuid=2a47b6ff-3a71-4054-a603-6e68aae51cfa&owner=fc5889a9-e049-442a-b208-b416f05e180d (accessed 13 March 2013).

Schomberg, R. (2011) *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (Brussels: Directorate General for Research and Innovation).

Spetalnick, M. and Holland, S. (2013) Obama defends surveillance effort as 'trade-off' for security, *Reuters*.

Stritzel, H. (2007) Towards a theory of securitization: Copenhagen and beyond, *European Journal of International Relations*, 13(3), pp. 357–383.

Valkenburg, G. and Van der Ploeg, I. (2015) Materialities between security and privacy: A constructivist account of airport security scanners, *Security Dialogue*, 46(4), pp. 326–344.

Van der Ploeg, I. (2005) Keys to privacy. Translations of 'the privacy problem' in information technologies, in: I. Van der Ploeg (Ed.) *The Machine-Readable Body. Essays on Biometrics and the Informatization of the Body*, pp. 15–36 (Maastricht: Shaker).

Vedder, A., Wees, L. v. d., Koops, B.-J., Hert, P. d., Harten, D. v. and Munnichs, G. (2007) *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw* (Den Haag: Rathenau Instituut).

Walters, W. (2014) Drone strikes, dingpolitik and beyond: Furthering the debate on materiality and security, *Security Dialogue*, 45(2), pp. 101–118.

WikiLeaks. (2011) 09BRASILIA1383, Brazil: Blackout—causes and implications, *Cables,* August 30.

Williams, M. C. (2003) Words, images, enemies: Securitization and international politics, *International Studies Quarterly*, 47, pp. 511–531.

Zureik, E. and Hindle, K. (2004). Governance, security and technology: The case of biometrics. *Studies in Political Economy*, 73, pp. 113–137.