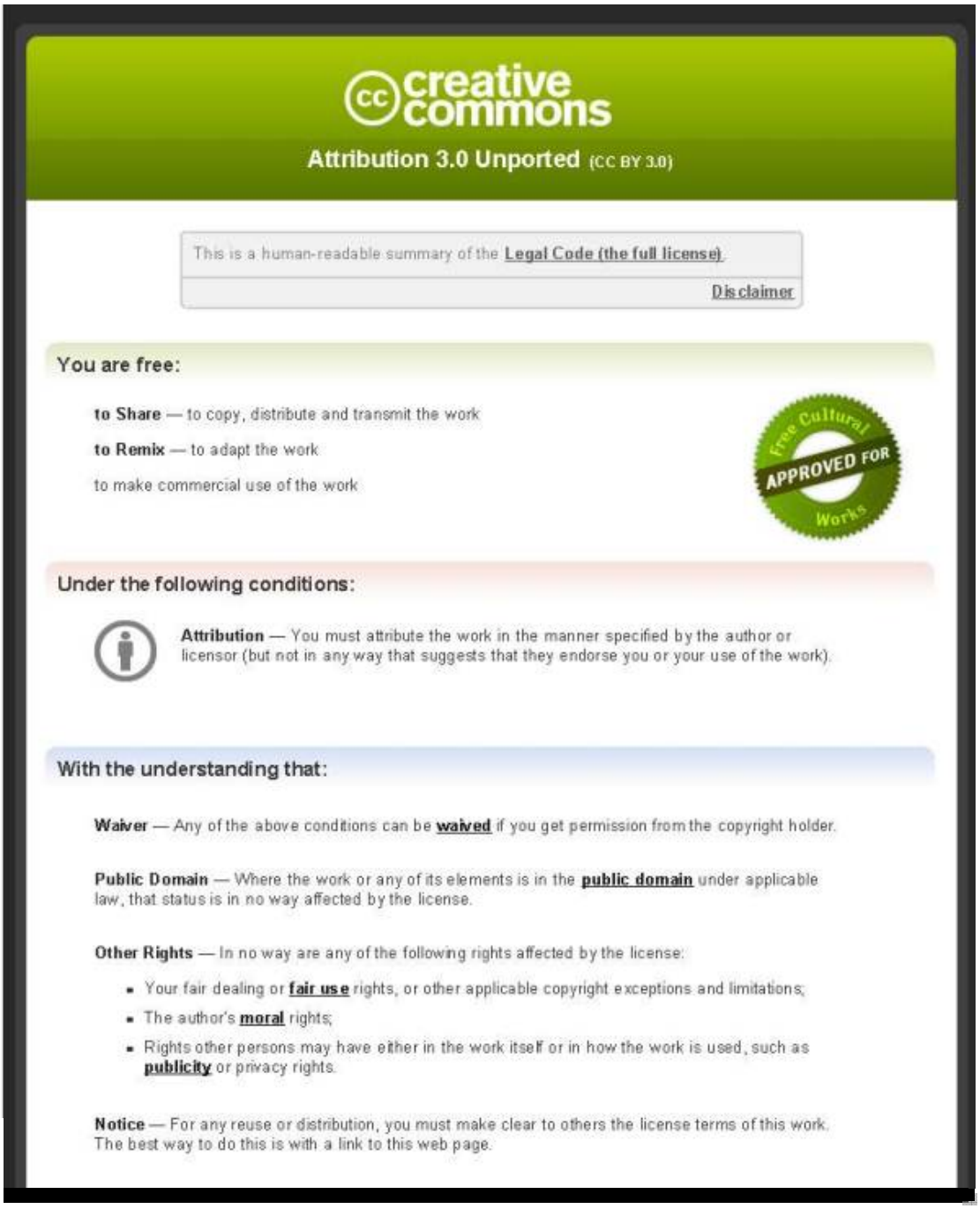

Information, Communication & Society
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/rics20

Confusion, control and comfort: premediating identity management in film and television

Georgina Turner[a], Liesbet van Zoonen[a] & Jasmine Harvey[b]
[a] Department of Social Sciences, Loughborough University, Brockington Building, Epinal Way, Loughborough, LE11 3TU, UK
[b] International Digital Lab, Warwick University, Loughborough, UK
Published online: 20 Dec 2013.

To cite this article: Georgina Turner, Liesbet van Zoonen & Jasmine Harvey (2013): Confusion, control and comfort: premediating identity management in film and television, Information, Communication & Society, DOI: 10.1080/1369118X.2013.870592

To link to this article: http://dx.doi.org/10.1080/1369118X.2013.870592

Information, Communication & Society, 2013
http://dx.doi.org/10.1080/1369118X.2013.870592

Confusion, control and comfort: premediating identity management in film and television

Georgina Turner[a]*, Liesbet van Zoonen[a] and Jasmine Harvey[b]

[a]*Department of Social Sciences, Loughborough University, Brockington Building, Epinal Way, Loughborough, LE11 3TU, UK;* [b]*International Digital Lab, Warwick University, Loughborough, UK*

(*Received 17 April 2013; accepted 25 November 2013*)

A number of national and international agencies have pointed to *identity management* (IM) as one of the main private and public challenges of the future. The issue is subject to intense public controversy and contestation, especially with respect to access to, usage and ownership of personal data. Most work about IM assumes users to be rational actors making instrumental choices on the basis of perceived usefulness and efficiency; cultural narratives hardly ever come up in current research about acceptance of new identity management technologies (IMTs). Screen representations do not prescribe certain meanings around IM, but create and delineate horizons of imagination; repositories of meanings from which people can draw to make sense of innovations and their consequences. In this paper, we focus on a sample of films, television and web series to examine how IMTs are premediated. Our analysis suggests that a whole range of future IM (knowledge- and token-based, as well as biometric/implant) technologies is imagined here, with biometric and implant technologies most likely to be taken to (dystopian) extremes. Stories of identity theft and confusion, surveillance and control, comfort and corruption construct them as potentially problematic and always under threat, as well as calling up existential concerns about what it means to be human. We conclude that these dark horizons are anchored in myth and persistent fears about who we are, and thus that new means of IM face a difficult task in gaining users' trust.

Keywords: identity management; premediation; future technologies; biometrics; science fiction; users' trust

1. Introduction

Everyday interactions increasingly require people to identify or authenticate themselves: when they draw cash from an ATM, when they use a customer loyalty card, or when they make online transactions. Likewise, medical check-ups, crossing national borders or acquiring certain licences involves procedures to introduce and prove one's identity. More and more, using objects and appliances necessitates the same: mobile phones can be pin-code protected, laptops may not start without a fingerprint scan, and office space may be biometrically secured. In the not-so-far future, smart homes could open on the basis of face recognition, and specific spaces such as the kitchen, bathroom or study are likely to become further personalized. People will be connected to such public and commercial services, to things and devices, and to each other, yet only if they are able consistently to identify and authenticate themselves to the network(s).

*Corresponding author. Email: g.turner@lboro.ac.uk

Hence the reliable, trustworthy and efficient management of offline and online identities is rapidly becoming a key challenge for individuals, as well as a significant issue in social policy and economic development. In fact, national and international agencies have pointed to *identity management* (IM) – which we can define as the identification and authentication of identities towards institutions, things and other people – as one of the main private and public challenges of the future (e.g. Camenisch, Fischer-Hübner, & Rannenberg, 2011; Gartner identifies, 2012; OECD, 2011). It is also an issue that is subject to intense public controversy and contestation, especially with respect to access to, usage and ownership of the personal data required for IM (cf. Bennett, 2010). In the UK in 2009, for instance, the government abandoned the national ID card scheme as a result of unresolved concerns around privacy and data protection (Whitley & Hosein, 2009). Likewise, in the Netherlands, the national electronic patient file was cancelled after public protest (Boonstra, Boddy, & Bell, 2008), and several states in the United States have developed legislation against the forced microchipping of persons (California bans, 2007).

The relationship between public(s) and (means of) IM is of significant research interest, but work in this emerging field has tended to focus on issues around privacy, data protection and civil liberties, and on the question of how to design secure and trustworthy IM systems (see Camenisch et al., 2011 for an overview). Where research has considered how people relate to, embrace, or reject, identity management technologies (IMTs) in everyday life (e.g. Byun & Byun, 2013; Clodfelter, 2010; Hossain & Prybutok, 2008; James, Pirim, Boswell, Reithel, & Barkhi, 2006; Sanquist, Mahy, & Morris, 2008; Smith, 2008), it has typically assumed the citizen or the consumer to be a rational actor, making instrumental choices on the basis of perceived usefulness and efficiency. To do so, though, ignores the cultural narratives that precede and interact with the technologies and the ways in which they are understood. Customer loyalty cards, for instance, not only facilitate an instrumental relationship between store and customer, but also express a sentimental bond of 'belonging' to a community (cf. Humby, Hunt, & Philips, 2008; brand communities also figure in Belk's, 1988/2013 notion of the extended self). Passports function mythically, as signifiers of national belonging *and* of cosmopolitanism (see van Zoonen, 2013). Meanwhile microchipping is bound up, conceptually, with the biblical metaphors – 'Mark of the Beast', and so on – successful mobilized by its opponents.

It thus seems imperative to consider, in addition to understanding rational considerations regarding the risks, benefits, ease and efficiency of IMTs, the cultural frameworks in which they exist. Here we focus on films, television and web series, not least because experts, journalists, activists and policy-makers regularly evoke screen stories and images to explain innovations and to describe their risks and opportunities. Kirby (2004, p. 184) says that the science fiction film *Gattaca* (1997), for instance, in which DNA screening has become the primary means of IM, has 'become a common reference point in discussions about human gene altering technologies'. Journalists use sentences such as: 'modern face-recognition technology conjures images of George Orwell's dystopian novel 1984' (Callahan, 2001). Privacy activists have used scenes from film and television to demonstrate what happens if the government or corporations have pervasive control of electronic identities: the Mall scene from Spielberg's *Minority Report* (2002) and the 'non-person' scene from the British series *The Last Enemy* (2008) both have been put on YouTube as part of privacy campaigns.

Such references are made on the assumption that the public will recognize the film in question, and that this recognition offers the potential to acquire a more vivid understanding of new IMTs. The literature from the sociology of technology uses the term 'leitbilder' to refer to such visions and popular imaginations (Borup, Brown, Konrad, & van Lente, 2006; Dierkes, Hoffman, & Maez, 1992). Some, termed 'placeholders', will remain in circulation far beyond the context of their original imagining (see Lösch, 2006). Highly popular titles or characters are most likely

to provide such visions – blockbusters like James Bond (and Q), *Minority Report* or the *Bourne* trilogy (2002) regularly fulfil such a function, as does George Orwell's *Nineteen Eighty Four* and the work of the science fiction writers Aldous Huxley, Philip K. Dick and William Gibson.

Grusin (2010) has argued that *all* media and genres are engaged in any case in the 'premediation' of our immediate futures. That is, in exploring the possible course that events, issues and technologies may take in a time span ranging from the next few days to the more distant future. News, popular culture and social media are no longer concerned with a representation of recent or live events, but are obsessing instead about what might happen next, whether it concerns the expected outcomes of the Arab spring, the possible solutions of the financial crisis or foreseen tornado damage. Several authors have taken up Grusin's concept of premediation, especially in the context of imagining security risks (e.g. De Goede, 2008). An issue such as IM, which is undergoing rapid technological progress, strong commercial push, and which involves contending political and social actors, will almost by definition continuously be 'premediated'.

The principle openness of premediation as imagining *all* possible futures, so that no particular one can come as a surprise, connects well with the generic codes and conventions of popular film and television: narrative structure, character construction, visual presentation and mode of address – in their potentially endless combinations – produce a 'text' that is by definition open to different interpretations. Such polysemy enhances audience appeal, and enables viewers to accommodate, negotiate or resist the meanings of the text (cf. Fiske, 1987). In any case, as Raven (2013) argues, there always exist multiple futures, each one's narrative exposition a recognizably subjective endeavour. Film and television thus do not prescribe certain meanings around IM, but create and delineate a so-called 'imaginative horizon' (Crapanzano, 2003), a repository of meanings and associations from which people can draw to make sense of innovations and their consequences. A privileged repository, at that, for experts and the wider public alike. It has been argued that one of the purposes of science fiction is to speculate – inviting its audience 'to ponder in some detail the effect that a given advance, change, discovery, or technological breakthrough might have' (Bretnor, 1974, p. 122; see also Scholes & Rabkin, 1977). So how are IMTs represented, how are their risks and potential constructed? Who benefits and suffers because of them? Evidently, if the repository does not contain contending ideas about the pleasures, desires, taboos, risks and opportunities of IMTs, it will be harder for members of the public to ponder scenarios beyond or outside of the horizon.

By analysing how IMTs are represented and framed on the screen, it is our aim to trace the horizon of imagination against which public understanding(s) of IMTs might be set.

2. The sample

Though we identified a focus away from cultural analysis in much of the work already to have addressed IMTs and their publics specifically, there exists a considerable body of work addressing surveillance technologies on screen. Kammerer (2002, p. 468) argues that

> in recent years, mainstream commercial cinema has seen an obvious trend to integrate the imagery and the aesthetics of video surveillance into the film itself, and/or to make the consequences, blessings or terrors (as the case may be) of a dooming "surveillance society" the subject matter of an entire movie.

It is standard for every contemporary police, crime or spy genre to show the use of global positioning system tracking, closed circuit television (CCTV) footage, data mining and other

surveillance technologies as common devices to solve and prevent crime or terrorism (cf. Lefait, 2012). The recent popularity of surveillance in cinema and TV has been widely identified as being the result of technological developments, the increased aura of realism that the representation of surveillance technology confers, and the double spectacle of watching someone being watched that it presents to audiences (cf. Kammerer, 2002). Almost all of these studies offer a broad-stroked cultural analysis, connecting surveillance cinema to wider societal processes such as the 'war on terrorism', but also self-surveillance on the internet, and reality television (e.g. Andrejevic, 2004; Lyon, 2007).

Surveillance cinema shows a range of IMTs (e.g. credit cards being tracked, CCTV with face recognition), yet it is of only partial relevance to a wider study of the cultural framework surrounding IM. While the realistic codes and conventions of such cinema draws audiences into their diegetic space to experience it as if they were part of it (Bordwell, 1985), they construct the IMTs and surveillance in particularly limited contexts of transgression. With respect to the 'horizon' for specifically imagining IMTs, we might reasonably say that the strong presence of surveillance narratives and visuals in modern and contemporary (and often primetime) film and television acts to close off more positive ideas and worlds. For a fuller understanding of the cultural framework that popular screen fiction offers about IM, however, we need to look beyond surveillance cinema and include a wider variety of genres and themes.

Using the Internet Movie Database (IMDb) to identify relevant titles – that is, films or series in which IM was a primary focus – we selected a sample of just over 80 titles, all released or aired after 1990 (see Appendix1). Basic information about each of these films was registered: a set of meta data (year of production, genre, time frame, medium, key themes and keywords tagged to the title); the means of IM present in the film, for which we used O'Gorman's (2003) categorization as knowledge- or memory-based means of IM (e.g. passwords or pin codes), object- or token-based (cards, passports), and body-based devices (biometrics, implants).

3. Findings

3.1. *General observations*

We focused our sample on the post-1990 period because relevant titles were rare before 1980, beginning gradually to increase, and then proliferating in the 1990s. This growth coincides with the birth and spread of the internet, bringing web-related titles such as *Sneakers* (1992), *Ghost in the Shell*, *Hackers*, *Johnny Mnemonic*, *The Net* (all 1995) and *The Matrix* trilogy (1999 on). The development of biometric technologies is taken up early in *Gattaca*, but especially in the 2000s, in films such as *Minority Report*, *Code 46* (2003), *A Scanner Darkly* (2006) and the *Bourne* series. Recent years have brought titles dealing with our increased dependence on online identification, such as *Identity* (2010), *H+* (2011) and *Cybergeddon* (2012). The latter two titles are web series, which have emerged recently and appear to be proliferating in the age of hyperconnectivity; most productions continue to be films, though television series are appearing with increasing frequency. As the debate continues as to whether or not television is supplanting film as the dominant art form and the natural place to examine society,[1] here we might wonder if television series encourage greater openness of the imaginative horizon: this is the format in which a longer narrative, combining any number of technologies, themes and contexts, can be sustained. In series such as *Spooks* (2002) and *Identity*, various protagonists face various enemies and must wrestle with their consciences, often rather conspicuously, on multiple occasions.

The key themes tagged most often to our titles proved to be 'mistaken identity', 'false identity', 'secret identity' and 'assumed identity', thus strongly suggesting that IM in film and

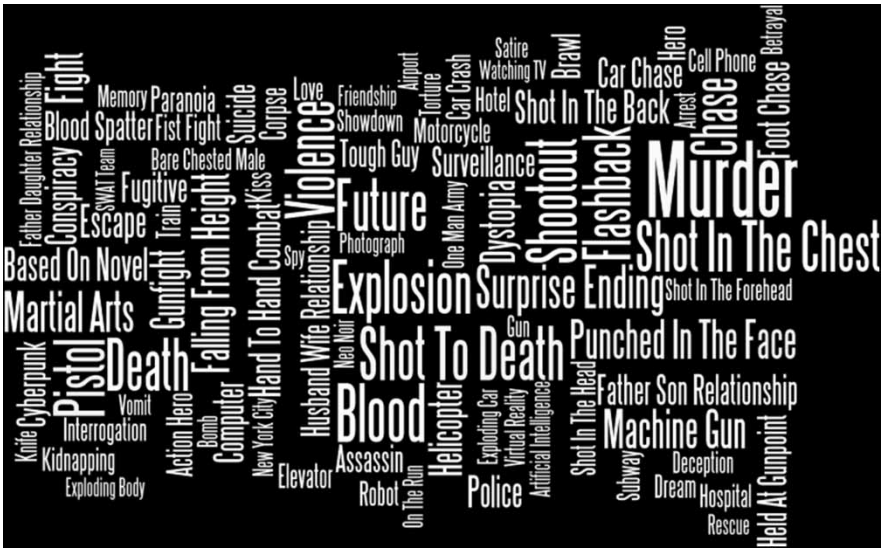

Figure 1. Visual representation of keywords. Tags applied to our sample of films on IMDb; overall the pattern is a negative and violent one.

television is usually associated with trouble. In order to sharpen these results, we submitted all tagged keywords pertaining to the films' content to Wordle, a piece of word-cloud freeware, to produce a visual representation of the 90 most frequently occurring keywords. Figure 1 (below) elaborates the negative pattern, showing how death, violence, pursuit and deception are also regularly tagged to IM films.

There are a number of similarities between these films and series in terms of the narratives they tell, the types of heroes and villains they involve, and the visual markers of tension and release. The classic works of Propp (1928) about fairy tales and Campbell about myths (1949) both suggest that there are only a limited number of similarly organized stories that people tell. The mythical heroic journey that both authors identify as a key driver of narrative is evidenced in Figure 1 by the presence of tags such as 'one man army', 'tough guy', 'fugitive' and so on. Invariably, as we will expand on below, an individual (e.g. Jason Bourne in the *Bourne* trilogy) or team (e.g. the MI5 operatives in *Spooks*) battles malevolent forces and leads the audience to some kind of triumph, however finite. The similarities seem to bear out irrespective of genre, though a majority of titles could, in any case, have been accommodated under several genres that we might amalgamate as 'action drama', with or without a science fiction bent (we have excluded the few comedy titles in the sample from this analysis, but these – and their relationship to the more common action dramas – are the subject of other work to be published). And, if we think of science fiction not just as aliens and spaceships but as fiction 'concerned with exploring the human consequences of technological development', as the filmmaker James Gunn put it (Turney, 2013), then even that differentiation becomes almost too slender. It is for this reason that we have not organized our findings according to genre.

Instead the discussion is structured around the aforementioned technology categories (knowledge-based, token-based and body-based) and will use examples from various titles to approach the questions scattered across our introduction: What tropes characterize their representation (and where/how/when, if ever, are these subverted)? Who benefits and suffers in these narratives and how do they construct risk and potential? How open or closed are they to various readings?

3.2. *Knowledge-based IMTs*

This is the system upon which many present-day interactions rely; we have pin codes for our credit and debit cards, passwords for our email accounts and security questions for online retail. There was a great deal of debate about the merits of chip-and-pin cards before and after they began to replace magnetic strips and signatures in the UK in 2004, concerning not only the impact on fraud (and liability) but also ease of use for disabled and elderly people confronted by increasing memory-based IMTs. 'We are living with a bewildering array of numbers to remember', wrote Barry (2004), in the Mirror. Research in the meantime has shown that even moderate computer users, regardless of age, are experiencing 'password overload', and can make poor or compromised choices in order to manage this (see, e.g. Notoatmodjo & Thomborson, 2009).

Knowledge-based IMTs such as pin codes and passwords are rarely a major theme in films and television shows in the way that, say, surveillance is. They are often, however, crucial plot points, and almost always because they fail. The success with which passwords are broken on screen is uncannily consistent, a well-worn trope that has been spoofed and hat-tipped since the 1930s.[2]

In *Code 46*, all citizens have a unique 'palabra' (Spanish for password) that permits them access to virtual and physical spaces. Using his virus-enhanced intuition, the male lead (William) discovers a receptionist's palabra, allowing him to wander freely around the offices of The Sphinx, and later uses his missing lover's palabra to access her apartment (the entry computer apparently not employing voice recognition). Only when he attempts to trick a hospital receptionist into revealing her palabra does he fail, because the (government-run) facility is protected from viruses such as the one he uses. There is evident ambiguity at here: William's trickery is unashamed and clearly causes his only knowing victim, the receptionist, a good deal of angst, yet he seems only to resort to using another's palabra 'for good' (i.e. to investigate a fraud, to find and rescue Maria).

This is reflected across our sample, as it is most common for the protagonist(s) – i.e. the 'good guys' – to be the ones to do the breaking. For example in *The Net* (1995), Angela Bennett has her own identity not only stolen but erased, yet she fights back using a password stolen from the wallet of the man contracted to kill her. In *Fortress* (1992) one of the prison escapees guesses Director Poe's username and password – his mantra 'Crime Does Not Pay' – in a single attempt, accessing the computer that controls the prison in order to upload a deadly virus. Passwords are more typically broken by a 'computer whizz' than by less technical characters who simply get lucky, however. Operatives in television programmes such as *Spooks*, *Hunted* and *24* have sophisticated gadgets to crack passcodes for them in a way that most people would be unable to replicate – though interestingly in *Identity*, which offers a comparatively realistic and down-to-earth take on the crime genre, a police officer attempts to decipher the password on a murdered teen's laptop manually, and fails.

So what we see is a strong perception of risk attached to memory-dependent IMTs – as viewers, we are accustomed to seeing them fail. This risk is coupled with the fact that 'the baddies' are so often the victims of a password-failure, but perhaps not quite offset by it; even if it usually takes resources beyond our own, it can and does happen to people like us. Indeed, after watching *Identity*, the Observer's reviewer wrote: 'I'm going to spend the rest of today changing my password to everything from what I thought was the rather clever "wordpass", and retrospectively altering my mother's maiden name to Pamplemousse'.

3.3. *Token-based IMTs*

This is, essentially, identity documented: driver's licence, passport, credit card, tube ticket – and in our films and shows is just as frequently falsified as memory-based IMTs. Again, however,

there is usually some level of expertise or professional capability involved; from the very beginning of the first film, the *Bourne* series relies on Jason Bourne's stash of fake ID (its location revealed in the first place by an implant in his hip), while in *RED* (2010) another (former) Central Intelligence Agency operative takes a sledgehammer to the foundations of his house, unearthing a box filled with cash and IDs. The fake documents here are a means of escape, aiding the impetus of the subsequent action, or allowing operatives in the spy-crime genre (e.g. *Spooks, 24*) to work undercover and stop the 'bad guys'.

That is not to say that we, as viewers, can always expect to find ourselves rooting for the fakers. *The Net*, released when less than 1% of the world's population had home internet access (and five years before the UK would have its first broadband customer), was one of the first films to address the vulnerability of our online identities, yet significant parts of the story hinge on physical identity tokens. Angela Bennett is vanished over the internet, but the theft of her handbag is critical. Without her travel documents, everyday identifiers or her credit card, she is unable to convince anyone – customs, the police, even neighbours – that she is Bennett and not Ruth Marx, a criminal alter-ego foisted upon her by cyber attackers. 'Ma'am, it would help if you could produce some form of identification', says a policeman. 'You know what? I agree with you', comes Bennett's sarcasm-tainted response. In her work on biometric identification, Ajana (2010, p. 240) writes that new technologies aim to 'purify' identification of human ambivalence and unreliability, and we see this reductive process explored in *The Net* and its sequal, *The Net 2.0* (2006). In the first film a senator commits suicide believing he has contracted AIDS after the cyberterrorists alter his blood test. Receiving the news, the senator asks, 'There's no chance a mistake could have been made? A misreading? Human error? It happens'. In fact what we see is quite the opposite: human interaction and intuition subverted and denied by automated systems and institutional dependence on, and deference to, IMTs: Bennett, and later Hope Cassidy, are both stuck in computer-says-no nightmares. Bennett's personal identity narrative (all she has left) is redundant: she fails to access her hotel room because the system tells the receptionist that she checked out three days earlier; she is able to re-enter the United States by signing for a visa as Marx even after having said that she was not Marx. Cassidy's identity narrative suffers a similar fate at the US Consulate, and where it survives it is hijacked along with her documents and used to vouch for the fake in her place. Like Bennett, over the course of the film her disbelief becomes despair. 'Do you realise what it feels like', she asks her interrogator, 'to go an entire life and realise that none of it matters? That basically the person you thought you were doesn't exist?'

The creator of *Identity*, Ed Whitmore, explicitly wanted his audience to 'realise what it feels like': 'We want the first episode to scare viewers and make them think, "That could happen to me"'. While the suspect uses false birth certificates, mocked up utility bills and a cloned driving licence to frame others for his crimes, the Identity Unit uses credit card transactions, Oyster cards, congestion charging receipts and discarded aeroplane tickets to try to identify their suspect. The tussle between 'good' and 'bad' is rendered explicitly as the operatives express their discomfort about how easily they can find the personal information of those involved in the investigation, yet rely on unpicking precisely those things to solve the case. As a suspect is identified through a rental car, one officer confirms that it was hired using proof of ID (driving licence) and paid for using a credit card. 'A transaction he vehemently denies', she adds, rolling her eyes as if the IMTs involved made this an utterly futile denial. From this complete faith in the technologies (they are central, after all, to her contribution to the team), a more mitigated stance is gradually negotiated: we may not be trapped by the say-so of IM tokens – at least not permanently.

It is interesting to consider the endurance of token-based IM, even where they routinely fail or can be faked or stolen. Even in highly futuristic settings in which other, more sophisticated

technologies dominate, identity tokens are still somehow integral. In *Brazil* (1985), for instance, seemingly independently mobile security cameras marshall the doors to the Ministry, yet Sam Lowry must show his ID every day as he arrives for work. The world of *Equilibrium* (2002) is heavily surveilled, and yet the cleric is reminded that 'unidentified individuals are subject to summary destruction' when he fails to produce an ID. And we return again to *Code 46*, where biometrics govern everything yet citizens must have a piece of paper, a 'papelle', in order to travel across continents and from 'outside' to 'inside'. There may be various reasons for this – they may well be simple plot points (*Code 46* requires something that can be faked in order to draw its protagonists together, and in *Brazil*, Gilliam's satire depends on it: Archibald Buttle is killed because his name appeared on the wrong piece of paper, and the intended victim, Archibald Tuttle, later drowns in a swirling storm of paperwork). Or these familiar items may work to anchor the narrative somewhere within our current frame of reference: there is in the twentieth and twenty-first centuries something solidly, tangibly *human* about 'things'. Declaring 2012 'the year that the password broke', Wired magazine reported in January 2013 that Google has plans to switch internet logins from memory-based to token-based technologies, on the basis that hardware can be held on to and kept from hackers. In *Dark City* (1998), aliens have complete biochemical control over the population, but also manufacture identification documents (diaries, photographs and letters), apparently recognizing in their human subjects some need for material testimony.

3.4. *Biometric/transhuman IMTs*

Increasingly, public discourse on the IMTs of the future focuses on biometrics; since the introduction to many countries of biometric passports in the mid-2000s, biometric technologies have carried what Neyland (2009, p. 136) calls 'a pervasive resonance', and have strongly divided opinion. The appropriateness and feasibility of biometric identification for certain purposes – national security, for instance – continue to be debated, yet there is generally an air of anticipation around reports that Apple is working with fingerprint recognition technology and that Sony plans to introduce biometric controllers that adjust gameplay in response to temperature and sweat.

In the films and television shows analysed, biometric IM, like memory– and token-based technologies, is routinely presented in a poor light: operational usually in a (future) surveillance state in which biometric identity is no longer an innovation but an institutionalized measure, and flawed as much for the difficulty with which it is subverted as for the fact that it may be subverted at all. It is in representing the future of biometric IM that we most often see the technology taken to its furthest logical conclusion before the action even begins. Viewers see not new technologies imagined, but new and expanded contexts and applications.

In *Gattaca*, for instance, blood tests are not only used to determine a person's identity in cases where it is the only (or only certain) way, but to permit access to buildings on a daily basis; in this society citizens are effectively graded from conception according to their genetic make-up. Their propensity for disease, life expectancy and predicted intelligence determines their life prospects, and constant genetic verification marshalls those restrictions in a system of macro and micro IM. Similarly, citizens in the world of *Code 46* are subject to constant genetic scrutiny, reliant on clearance from The Sphinx to marry and procreate as well as to travel. Gone are present-day, real-world fears about the effects of cloning and in their place a world full of clones, their genes social determinants.

As in *Minority Report*, where a black market in eyeballs facilitates those wishing to avoid the constant retinal scanning that serves government and commercial paymasters, *Gattaca* predicts the commodification of genetic identity. One character bound to an 'invalid' life by his genes (Vincent) purchases the genetic markers of another equally bound by the expectations of his

'valid' identity (Jerome), and our sympathies are eked out by both as they seek to manage their own destiny in a dehumanized system. Each person is reduced to their DNA, so much so that when Vincent worries that the plan is doomed to fail because he does not resemble Jerome, the 'fixer' poses a striking rhetorical question: 'When was the last time anybody looked at a photograph?' Jerome and Vincent both speak to police officers *as Jerome*, yet neither the physical difference nor their different accents appears to cause any trouble. Vincent lives as Jerome because the pocket of Jerome's blood he attaches to his index finger every morning tells a computer that he is Jerome.

Again, then, we find some anxiety in relation to the level of faith placed in these technologies at the expense of human understanding and interaction. Though an attempt to use a severed alien arm to operate a weapon fails in *District 9* (2009), in *Demolition Man* (1993), Simon Phoenix succeeds in using a recently removed eyeball (hanging grimly off the end of a pen) to fool a retina scanner, just as John Anderton does in *Minority Report*.[3]

The (imagined) future merging of bodies and technologies also presents particular problems. In the web series *H+*, the majority of the world's adult population is implanted with a wireless device that networks with the central nervous system, allowing constant online interactivity viewed on a floating virtual interface. Presented in brief episodes released on YouTube, the series is very much of its time, and the first part of the first episode does a great deal of work in helping the viewer to make the leap from today to the world of H+: clips from standard-looking rolling news broadcasts describe the implant's evolution from a medical device to a personal networked computer operated by and within the body.

In terms of production and aesthetics, the series at this stage shares a lot of similarities to the kinds of realistic television series mentioned earlier, setting up the sudden transition in to the time of a catastrophic event: a virus communicated over the worldwide network that kills everyone connected. If an implanted computer is difficult to envisage (one short film from 2012 featured a similar interface produced by a contact lens, and in the real-world Google Glass is probably as close as we have come), the intermediate stage at which the computer is a medical intervention may be important; we are becoming accustomed to seeing developments in medical technologies. Supporting the imaginative process, scenes are cut together with computer generated synapses; glowing green on black backgrounds like the monochrome monitors of the 1980s, sound effects twitching and fizzing like loose cables. Just as CCTV-type shots are used in surveillance films (Lyon, 2007), these images can immerse the viewer in the technology. Once we can imagine our bodies as fleshy computers, it is a simple step to imagining a risk such as a virus.

4. Themes: confusion, control and comfort

Overall we see a body of work that is nervous about the future and what it holds for our identities: films and TV series of various kinds highlight especially the potential problems and risks attached to IM. The titles we considered routinely imagine that the three current forms of IM will still exist in the future, and that the memory- and token-based forms of IM will continue to be easily falsified and compromised. Biometric and implanted means of IM are imagined as being more secure, but also, and often for that very reason, as being riskier in the wrong hands. Across the sample there is a fundamental ambiguity around instruments of IM, because they are used and abused by protagonists and antagonists alike; their strengths are weaknesses, and vice versa. Viewers are seemingly encouraged to ponder, if not interrogate, the very notion of protagonists and antagonists, sometimes in the same titles. In *Code 46*, both principle characters flit from one position to the other *as part* of the struggle inherent in coping with their storyworld. This and other ambiguities play out in (and across) three central themes: confusion, control and comfort.

4.1. *Confusion*

Identity theft (in its various guises) and mistaken identities figure prominently in our films – with the resulting angst and confusion often a, if not the key, driver of the film's narrative. 'Confusion' manifests in various ways, from the protagonists who are suffering some kind of personal existential crisis to those who (also) question the identities of others. The particulars of these nightmares are, often, uniquely the characters'. The producers of *The Net* films, for instance, had to go to some length to contrive situations in which lead characters could be vanished: Bennett is reclusive with a senile mother who does not recognize her; Cassidy has no living family and has just arrived in Istanbul, where she knows nobody. The average person does not tend to fear discovering that our world is simulated, as Neo does in *The Matrix*. We are unlikely to be dragged out of the ocean with no recollection of who we are, and even less likely to discover that an implanted chip can direct us to a safe deposit box filled with the identity documents of our various personas (*Bourne*). Yet it requires no great leap of imagination to empathize with the helplessness, anxiety and uncertainty – the confusion – bound up in these stories. That these players – protagonists and antagonists alike – often are not 'average Joes' is open to multiple interpretations. Is our own web presence reassuringly small? Or do we begin to wonder: 'If it can happen to these guys … '

4.2. *Control*

As the literature about surveillance cinema suggests, we find IMTs in film and television series often deployed as instruments for surveillance by the state. The quintessential story here is, of course, George Orwell's *Nineteen Eighty Four*, which was made into a film for the first time in 1956, and remade in the year 1984 itself. The theme has been worked and reworked in films such as *Alphaville* (1965) and *Brazil* (1985), and in our sample we find, among others, *V for Vendetta* (2005), *Gattaca*, *Equilibrium* and *Eyeborgs* (2009) exploring current and more high-tech forms of state oppression. Increasingly, we see other powerful and all-seeing forces than the state come up in these stories. In *Hunted* we meet agents working for a private security company, and the plot, revolving around falsified identities, involves a conspiracy of the five biggest corporations of the world. *Continuum* fast-forwards to 2077, a time in which governments no longer exist and the population relies for all resources upon vast companies to whom they are, essentially, always indebted, working for credits to be redeemed. Corporate power is thus emerging as a force as oppressive as the state, possessing similar powers of surveillance and control. Based on what we see on our screens, surveillance is inescapable and blind to nuance. Significantly, in a number of our selected titles, even those doing the surveillance are subjected to its risks and become victims of its ubiquity. In *Fortress*, the prison director is eventually destroyed by the surveillance system's automated weapons, while in *Minority Report* the protagonist John Anderton is quickly on the run from his own PreCrime unit.

4.3. *Comfort*

Alongside (in fact intertwined with) concerns about control often comes a sense of comfort: in numerous titles IMTs are pervasive, even intrusive, but are successfully deployed to protect people from crime. Technologies might pose questions about the meaning and value of privacy and the social contract, but in identifying victims and tracking perpetrators, they perform a positive role. The main characters in such series are no less than heroic in their drive to help and protect ordinary citizens, often at a great personal cost. Thus, Jack Bauer in *24* and the MI5 agents in *Spooks* have no private life to speak of; the Crime Scene Investigators routinely become so obsessed with their case that they forget everything else, including their family

obligations; and the *Person of Interest* protagonists seem perfectly happy to be officially non-existent, so that they can fulfil their duties to humanity.

By definition of the codes of mainstream film and television, in the end the good guys will win. However, with the increasing complexity of film and television series (see Johnson, 2006), these are not always simply happy endings. In part because another threat is always looming, and also because the heroes are frequently compromised in the process. Certain individuals set a reassuring moral high-water mark (e.g. Sir Harry Pearce in *Spooks*), but with high-stakes battles the protagonists in numerous titles face some kind of moral dilemma. At times such moments break key players: in *H+* for instance, the inventor of the implant technology becomes so disillusioned with what the company wants to do with it that he abandons his contract. At others an, 'It's a dirty job but someone has to do it' mantra is required.

5. Discussion

It is not simply the case that some titles dwell on concerns about control (Who is in control? How much autonomy do I have?) while others focus on human confusion (Who am I? Who are they?); these issues are as bound up with one another as they are with the technologies involved. The confusion aroused by identity theft and manipulation, the fears about control and individualism provoked by surveillance narratives: these things are not vanished by any comfort we draw from seeing bad guys get their comeuppance. Concern and consolation co-exist; mingle; fight one another for the foreground. *Identity* captures this in a single line, uttered when the team uses London's congestion charging cameras to track down a father in order to inform him of the death of his daughter: 'You can beat me with the civil liberties stick later'.

In the course of imagining the future of IM systems and devices, these stories probe complex social and moral issues and call up existential concerns about what it means to be a human being, how to live with others and to whom (or what) to defer control. While individual films and TV series may answer those questions differently, taken (momentarily) as a package they construct IMTs as potentially problematic and always under threat of corruption by individual and collective actors – sometimes precisely because of the good that can be done with them. Messages about the resilience of the human spirit (signified, say, by the reassuringly common sight of some kind of resistance, or the certainty with which a protagonist maintains a sense of self in spite of swirling confusion as to how to prove it) undercut the otherwise pervasive sense of the inevitability and proximity of a dystopian future. Yet their effects often feel temporary, merely a deferment.

If we return to our purpose in analysing this package, as a repository of meaning from which the public can build their understandings of and feelings towards existing, novel and future IMTs, these trends are important. Particularly when one considers that these types of concerns have always played out in popular narrative: classic mythology, for instance, is rife with gods and demi-gods who disguise themselves as others (see Murnaghan, 1987); pre-modern folklore similarly abounds with stories about imposters, impersonation and identity fraud (e.g. Davis, 1983; Williamson, 1957); modern urbanization created anxieties about who all these fellow-urbanites were and whether they could be trusted, which resulted, according to Boltanski (2012), in the emergence of the detective novel, as exemplified by the stories of *Sherlock Holmes.* These films and television series are a contemporary articulation of permanent tropes in human storytelling, the latest iteration of a set of fundamental concerns, in which new technologies and social realities are entangled. It is too mechanical to attribute recent policy failures simply to popular film and television narratives; instead we see them as having a strong mythical dimension, expressing 'basic concerns, core values, deep anxieties' (Silverstone, 1988, p. 24). These narratives are themselves anchored in much older, and persistent, existential fears about who we and others are, how we can trust what we see, and how society should manage all of this uncertainty.

And in this context we must conclude that the trust of users in new means of IM will not come easily but will always need to be actively acquired and deserved.

Notes

1. See, for example, David Cox's discussion: http://www.theguardian.com/film/filmblog/2013/jun/24/before-midnight-film-tv
2. In *Horse Feathers* (1932), Chico Marx unwittingly divulges the secret password ('swordfish') to a speakeasy to Groucho; swordfish has subsequently featured as the password in numerous films and television series, including *The Net* and *Hackers* (both 1995).
3. This kind of scenario was well spoofed by the little-known US cartoon Stroker and Hoop in 2005, when Stroker broke into a facility using an unconscious guard's handprint and urine, only to be apprehended by another guard inside who had watched the whole thing on camera. *But you're supposed to be reading a magazine or watching the game!*

Notes on contributor

Georgina Turner is a research associate in the Department of Social Sciences at Loughborough University. Her interests are media representations and discourses (and their production and consumption), identity in its personal, social and collective senses, and the use of multiple and innovative methodologies. [email: g.turner@lboro.ac.uk]

Liesbet van Zoonen is a professor of Communication and Media Studies at Loughborough University, and professor of Popular Culture at Erasmus University Rotterdam. Her work covers the articulation of popular culture and politics, for which she uses a wide range of standard and creative quantitative and qualitative methodologies. [email: e.a.van-zoonen@lboro.ac.uk]

Jasmine Harvey is a research fellow at the University of Warwick's International Digital Lab, working on healthcare information technologies and digital services. She was previously a research associate at Loughborough University. [email: jasmine.harvey@warwick.ac.uk]

References

Ajana, B. (2010). Recombinant identities: Biometrics and narrative bioethics. *Journal of Bioethical Inquiry*, *7*(2), 237–258. doi:10.1007/s11673-010-9228-4

Andrejevic, M. (2004). The webcam subculture and the digital enclosure. In N. Couldry & A. McCarthy (Eds.), *MediaSpace: Place, scale and culture in a media age* (pp. 193–208). London: Routledge.

Barry, M. (2004). 'Chip & pin puts us on fast track to button gloom' Daily Mirror. Retrieved from http://www.thefreelibrary.com/Maggie+Barry%3A+Chip+%26+Pin+puts+us+on+fast+track+to+button+gloom.-a0121633778

Belk, R. (1988). Possessions and the extended self. *Journal of Consumer Research*, *15*, 139–168. Retrieved from http://www.jstor.org/stable/2489522

Belk, R. (2013). Extended self in a digital world. *Journal of Consumer Research*, *40*. doi:10.1086/671052

Bennett, C. (2010). *The privacy advocates: Resisting the spread of surveillance*. Cambridge, MA: MIT Press.

Boltanski, L. (2012). *Énigmes et complots: Une enquête à propos d'enquêtes*. Paris: Editions Gallimard.

Boonstra, A., Boddy, D., & Bell, S. (2008). Stakeholder management in IOS projects: Analysis of an attempt to implement an electronic patient file. *European Journal of Information Systems*, *17*(2), 100–111. doi:10.1057/ejis.2008.2

Bordwell, D. (1985). *Narration in the fiction film*. Madison, WI: University of Wisconsin Press.

Borup, M., Brown, N., Konrad, K., & van Lente, H. (2006). The sociology of expectations in science and technology. *Technology Analysis & Strategic Management*, *18*(3/4), 285–298. doi:10.1080/09537320320000046024

Bretnor, R. (Ed.). (1974). *Science fiction today and tomorrow*. New York: Harper Row.

Byun, S., & Byun, S. E. (2013). Exploring perceptions toward biometric technology in service encounters: A comparison of current users and potential adopters. *Behaviour and Information Technology*, *32*(3), 217–230. doi:10.1080/0144929X.2011.553741

California bans forced RFID tagging of humans (2007, October 17). *Government technology.* Retrieved from http://www.govtech.com/security/California-Bans-Forced-RFID-Tagging-of.html?topic=117688
Callahan, D. (2001, June 22). Overmatched by technology. *The Washington Post*, np.
Camenisch, J., Fischer-Hübner, S., & Rannenberg, K. (Eds.). (2011). *Privacy and identity management for life*. New York: Springer Press.
Campbell, J. (1949). *The hero with a thousand faces*. New York: Pantheon Books.
Clodfelter, R. (2010). Biometric technology in retailing: Will consumers accept fingerprint authentication? *Journal of Retailing and Consumer Services*, *17*(3), 181–188. doi:10.1016/j.jretconser.2010.03.007
Crapanzano, V. (2003). *Imaginative horizons: An essay in literary-philosophical anthropology.* Chicago, IL: University of Chicago Press.
Davis, N. Z. (1983). *The return of Martin Guerre*. Cambridge: Harvard University Press.
De Goede, M. (2008). Beyond risk: Premediation and the post-9/11 security imagination. *Security Dialogue*, *39*(2–3), 155–176. doi:10.1177/0967010608088773
Dierkes, M., Hoffman, U., & Maez, L. (1992). *Leitbild und Technik: Zur Entstehung und Steuerung technisher Innovationen*. Berlin: Edition Sigma.
Fiske, J. (1987). *Television culture*. London: Methuen.
Gartner Identifies Six Trends That Will Drive the Evolution of Identity and Access Management and Privacy Management in 2012 (2012, January 31) *Gartner.* Retrieved from http://www.gartner.com/it/page.jsp?id=1909714
Grusin, R. A. (2010). *Premediation: Affect and mediality after 9/11*. Basingtstoke: Palgrave MacMillan. *Premediation: In which I attempt to think through the concept of premediation on the fly.* Retrieved from http://premediation.blogspot.nl
Hossain, M. M., & Prybutok, V. R. (2008). Consumer acceptance of RFID technology: An exploratory study. *IEEE Transactions on Engineering Management*, *55*(2), 316–328. doi:10.1109/TEM.2008.919728
Humby, C., Hunt, T., & Philips, T. (2008). *Scoring points: How Tesco continues to win customer loyalty.* London: Kogan Page.
James, T., Pirim, T., Boswell, K., Reithel, B., & Barkhi, R. (2006). Determining the intention to use biometric devices: An application and extension of the technology acceptance model. *Journal of Organizational and End User Computing*, *18*(3), 1–24. doi:10.4018/joeuc.2006070101
Johnson, S. (2006). *Everything bad is good for you: How today's popular culture is actually making us smarter*. London: Penguin.
Kammerer, D. (2002). Video surveillance in Hollywood movies. *Surveillance & Society*, *2*(2/3), 464–473. Retrieved from http://www.surveillance-and-society.org/cctv.htm
Kirby, D. A. (2004). Extrapolating race in GATTACA: Genetic passing, identity, and the science of race. *Literature and Medicine*, *23*(1), 184–200. Retrieved from http://muse.jhu.edu/journals/literature_and_medicine/toc/lm23.1.html
Lefait, S. (2012). *Surveillance on screen: Monitoring contemporary films and television programs*. Plymouth: Scarecrow Press.
Lösch, A. (2006). Anticipating the futures of nanotechnology: visionary images of means of communication. *Technology Analysis and Strategic Management*, *18*(3/4), 393–409. doi:10.1080/09537320600777168
Lyon, D. (2007). *Surveillance studies: An overview.* Cambridge: Polity Press.
Murnaghan, S. (1987). *Disguise and recognition in the Odyssey.* Princeton: Princeton University Press.
Neyland, D. (2009). Who's who? The biometric future and the politics of identity. *European Journal of Criminology*, *6*(2), 135–155.
Notoatmodjo, G., & Thomborson, C. (2009). Passwords and perceptions. In L. Brankovic & W. Susilo (Eds.), *Proceedings of the seventh australasian conference on information security* (Vol. 98, pp. 71–78). Darlinghurst: Australian Computer Society.
OECD. (2011). *Digital identity management: Enabling innovation and trust in the internet economy.* Retrieved from http://www.oecd.org/internet/interneteconomy/49338380.pdf
O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, *91*, 2019–2020. doi:10.1109/JPROC.2003.819611
Propp, V. (1928/1968). *Morphology of the folktale*. Texas: University of Texas Press.
Raven, P. G. (2013, July). *Worlds that tell stories, stories that tell worlds: Diegesis and mimesis in science fiction and technoscience.* Paper presented at Science in Public 2013, University of Nottingham, Nottingham.
Sanquist, T., Mahy, H., & Morris, F. (2008). An exploratory risk perception study of attitudes toward homeland security systems. *Risk Analysis*, *28*, 1125–1133. doi:10.1111/j.1539-6924.2008.01069.x
Scholes, R., & Rabkin, E. S. (1977). *Science fiction: History, science, vision*. Oxford: Oxford University Press.

Silverstone, R. (1988). Television myth and culture. In J. Carey (Ed.), *Media, myths and narrative: Television and the press* (pp. 20–47). London: Sage.
Smith, A. D. (2008). Evolution and acceptability of medical applications of RFID implants among early users of technology. *Health Marketing Quarterly*, *24*(1–2), 121–155. doi:10.1080/07359680802125980
Turney, J. (2013). *Imagining technology* (Nesta Working Paper No. 13/06), Nottingham.
Whitley, E., & Hosein, G. (2009). *Global challenges for identity politics*. Basingstoke: Palgrave MacMillan.
Williamson, H. R. (1957/2002). *Who was the man in the iron mask? and other historical enigmas*. London: Penguin Classics.
van Zoonen, L. (2013). Reflections on a passport. In P. Bennett & J. McDougall (Eds.), *Barthes' mythologies today: Readings of contemporary culture* (pp. 80–85). London: Routledge.

Appendix 1.

Title	Year	Setting	Form
Fortress	1992	Future	Film
Sneakers	1992	Present	Film
Demolition Man	1993	Future	Film
Ghost in the Shell	1995	Future	Film
Hackers	1995	Present	Film
Johnny Mnemonic	1995	Future	Film
The Net	1995	Present	Film
Virtuosity	1995	Future	Film
Mission Impossible	1996	Present	Film
Double Team	1997	Present	Film
Gattaca	1997	Future	Film
Men in Black	1997	Present	Film
Dark City	1998	Present	Film
Enemy of the State	1998	Present	Film
The Truman Show	1998	Present	Film
Edtv	1999	Present	Film
Existenz	1999	Future	Film
The Matrix	1999	Future	Film
The Talented Mr Ripley	1999	Present	Film
Fortress 2	2000	Future	Film
The Manchurian Candidate	2000	Future	Film
The 6th Day	2000	Future	Film
24	2001	Present	TV
A.I.	2001	Future	Film
Impostor	2001	Future	Film
Replicant	2001	Present	Film
Catch Me If You Can	2002	Present	Film
Cypher	2002	Future	Film
Equilibrium	2002	Future	Film
Minority Report	2002	Future	Film
S1mOne	2002	Present	Film
Spooks	2002	Present	TV
The Bourne Identity	2002	Present	Film
Code 46	2003	Future	Film
Natural City	2003	Future	Film
Paycheck	2003	Present	Film

(*Continued*)

Appendix 1. Continued.

Title	Year	Setting	Form
The Matrix Reloaded	2003	Future	Film
The Matrix Revolutions	2003	Future	Film
I, Robot	2004	Future	Film
Battlestar Galactica	2004	Future	TV
The Bourne Supremacy	2004	Present	Film
The Final Cut	2004	Future	Film
The Incredibles	2004	Present	Film
Kiss Kiss Bang Bang	2005	Present	Film
The Island	2005	Future	Film
V for Vendetta	2005	Future	Film
A Scanner Darkly	2006	Future	Film
The Lives of Others	2006	Past	Film
Identity Theft	2007	Present	Film
The Bourne Ultimatum	2007	Present	Film
Babylon AD	2008	Future	Film
Eagle Eye	2008	Future	Film
Get Smart	2008	Present	Film
Sleep Dealer	2008	Future	Film
The Last Enemy	2008	Present	TV
Caprica	2009	Unknown	TV
District 9	2009	Present	Film
Eyeborgs	2009	Future	Film
Gamer	2009	Future	Film
Identity Theft	2009	Present	Film
Surrogates	2009	Future	Film
Inception	2010	Future	Film
Red	2010	Present	Film
Salt	2010	Present	Film
Identity	2010	Present	TV
H+	2011	Present	Web
Black Mirror	2011	Present	TV
In Time	2011	Future	Film
Source Code	2011	Future	Film
Unknown	2011	Present	Film
Person of Interest	2011	Present	TV
Cybergeddon	2012	Present	Web
Memorize	2012	Future	Web
Homeland	2012	Present	TV
Hunted	2012	Present	TV
The Bourne Legacy	2012	Present	Film
The Hunger Games	2012	Future	Film
The Scapegoat	2012	Past	Film
Sight	2012	Future	Web
Continuum	2012	Split	TV
Identity thief	2013	Present	Film