March 23, 2009

Technology and the Crime Society: Rethinking Legal Protection

Bert-Jaap Koops, *Tilburg University*

Technology and the Crime Society: Rethinking Legal Protection

Bert-Jaap Koops[*]

Abstract

Building on existing insights of the risk society and the surveillance society, this article sketches the contours of the emerging crime society, where every form of human behaviour is perceived in terms of potential criminal risk and controlled by means of criminal law. It articulates the pivotal role of technology in the ever increasing footprint of criminal law, as it often facilitates criminalisation, expanding policing, preventative and architectural approaches, and pervasive surveillance. Criminal law is shifting from a last resort to a primary tool of social control: criminal risk governance. This paradigm shift goes hand in hand with a shift in the power balance between government and citizens, not the least because of the unlimited and relentless storage, data mining, and memory capacities of data bases. Therefore, we have to rethink legal protection for citizens. Apart from continuing to ensure a balanced investigation of concrete crimes and a fair trial, the advent of the crime society also calls for embedding organised distrust throughout the criminal justice system, by additional, systematic auditing and administrative controls.

Key words

criminal law, technology, surveillance society, risk society, legal protection

Contents

1 Introduction

In May 2003, in Vienna, a salt cellar was stolen that was worth some 45 million euros (it happened to be a masterpiece by Benvenuto Cellini). The perpetrator tried to sell the salt cellar back for ransom, but at the last moment, he sent an sms to call the transaction off. Through this phone number, the police were somehow able to find out the place where the mobile phone had been bought, the shop turned out to still have video tapes of the moment the phone was sold, an image of the man was broadcast, he was recognised by

[*] Prof.dr. Bert-Jaap Koops has an M.Sc. in mathematics, an M.A. in literature, and a Ph.D. in law. He is professor of regulation and technology at TILT, the Tilburg Institute for Law, Technology, and Society, of Tilburg University, the Netherlands. This article was written as part of a project on law, technology, and shifting balances of power, funded by the Netherlands Organisation for Scientific Research.

acquaintances and caught soon afterwards. The perpetrator confessed and led the police to a forest near Zwettl where he had buried the precious salt cellar.[1]

This wonderful piece of sleuthing shows the enormous value that information technology has brought to policing: phone records and video images were the key to finding the perpetrator. It is by no means exceptional, and similar stories can be told about technological advances in, for example, chemical, financial, and DNA forensics. Technology has an enormous enabling potential for solving crimes. But is does more than that. Technology opens up new horizons for information collection, and it enables monitoring, profiling, and predicting human behaviour, thus facilitating crime prevention alongside crime repression in hitherto unknown ways.

With its potential to collect and connect information, technology reinforces a social trend of growing desires to control people and society in order to minimise risks as much as possible. Crime is a primary risk in the perception of people and politicians alike, and criminal law has evolved into a powerful tool for governing social problems.

In this article, I will show that the combined trends of ever increasing technological potential, risk management, and governance through crime lead to what I would like to call a 'crime society'. The crime society is a society pervaded by crime-thinking and crime-fighting; a society with an ever larger footprint of criminal law, both substantively in the types of behaviour that are criminalised, and procedurally in expanding policing powers and changing societal architecture for the sake of crime control. In all of these processes, technology plays a pivotal facilitating role.

My aim in this article is twofold. First, I want to describe this process of 'criminalisation' of society and to articulate the role of technology in this. Although it is by no means the only relevant factor, I hope to show that technology is a crucial facilitating factor here. The combination of technology and the increasing footprint of criminal law has received relatively little attention in the literature to date. Most literature on the risk and surveillance societies mentions technology as a pivotal factor, but does not focus in particular on the increasing role of criminal law. Conversely, most literature on criminalisation and penal harshness tends to focus on increasing punishment and incarceration, but not on the technology-facilitated shadow that criminal law casts on human behaviour before it reaches, if it ever does, the stage of criminal conviction and punishment. I will therefore start with describing today's technological and socio-political contexts and outline how these jointly pave the way for a crime society. I will argue that this development effectively constitutes a paradigm shift towards viewing criminal law as a first resort rather than, as it used to be in legal doctrine, an *ultimum remedium*.

Second, I want to highlight one aspect of this development: the need for rethinking legal protection. What, in a crime society, is the role of the law in protecting individuals against abuse of power by those in control? I will argue that the paradigm shift in criminal law forces us to reconsider the way in which we construct legal protection. Quite possibly, a paradigm shift is required in legal protection as well, and I will outline some contours that in my view need to be part of the new paradigm.

Thus, the research question that is central to this article can be phrased as: what are the implications of the technology-facilitated criminalisation of society for the legal protection of citizens?

The trends described in this article are quite general; technology in itself is usually global in nature, and an increasing footprint of criminal law can be perceived in most Western countries. Although my line of argument may therefore be of general interest, I will illustrate my description and analysis with references to three countries in particular: the United States, the United Kingdom, and the Netherlands. I have chosen these countries because the trends perceptible there are exemplary for my argument, because several elements of the move towards a crime society in these countries are well documented,[2] and because it is interesting to elucidate the consequences for legal protection for both Anglo-American and Continental legal systems. The aim of this article is not to provide a comprehensive overview of all

[1] 'Strange case of the £35m saltcellar', *Guardian* 23 January 2006, http://www.guardian.co.uk/artanddesign/2006/jan/23/arttheft.austria (last visited 19 February 2009).

[2] See, for example, D. Garland, *The culture of control: crime and social order in contemporary society* (Chicago: University of Chicago Press 2001), J. Simon, *Governing through crime: how the war on crime transformed American democracy and created a culture of fear* (Oxford ; New York: Oxford University Press 2007), M. Cavadino and J. Dignan, *Penal systems: a comparative approach* (London: SAGE 2006), and A.H. Vedder, et al., *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw* (Rathenau Instituut, 2007), and other literature mentioned *infra*, sections 3 and 4.

technology-related criminal developments in these countries, nor to investigate the precise national similarities and differences. Instead, I will use illustrative examples from the three countries that, together with existing literature, underpin a general argument about technology, the crime society, and legal protection. This largely theoretical argument can serve as an hypothesis which subsequent, more detailed and empirical, research can try and corroborate, refute, or differentiate.

2 Technological Context

In this and the next section, I will sketch the technological and social contexts in which the move towards a crime society takes place. To show the interplay between both contexts and criminal law, I will highlight major trends and illustrate these with examples relevant to criminal law. I start with the technological trends. These started already in the 1960s and 1970s with the rise of computers and automated data processing, but they have accelerated in the 1990s and 2000s both in scale and in kind, and I will therefore focus largely on the more recent trends in technology.

2.1 Ever More Data

There are varying trends in technology that help law enforcement. These have one common denominator: technology leads to ever more data that are generated, processed, and stored. There is a twofold difference: data increase both in kind and in quantity.

First, over the past decades, *types* of data have become available that hitherto did not exist, or that have never before been stored. Various mechanisms are at work here. Objects become identifiable through a unique number or code. Expensive objects like soccer world cup tickets or cows are equipped with unique radio-frequency identitication (RFID) chips,[3] and this trend may continue with cheaper consumer goods; computers are made uniquely identifiable to enable 'trusted computing'[4]. Moreover, objects appear identifiable as technology discovers unexpected unique characteristics: computers[5] and cameras[6] apparently also have 'fingerprints', and even paper may be recognisable through a unique grain pattern.[7] In short, the identity of many individual goods – which may point to individual suspects – becomes known. The same holds for persons themselves: identifying data have emerged as a crucial new data category, through biometrics, centralised and multi-purpose identification numbers and ID cards, and compelled registration of identities through, for example, know-your-customer laws. And like objects, also persons can be RFID-chipped, not only in the Baja Beach Club, but also for tracking convicts or vulnerable children or elderly people.[8]

Another key type of new data that is emerging are location data. Telecommunications networks know where mobile phones are, and objects with GPS or Galileo equipment know their own location through satellite measurements. This enables the booming market of location-based services as well as road-pricing and public-transport pricing, but also (perceived) security-enhancing measures like legislation for mandatory locatability of mobile phones that call emergency numbers, or insurance companies mandating cars to be equipped with tracers.[9] There are even proposals for mandatory authentication of computers

[3] *See* on RFID, eg, http://www.rfidconsultation.eu/ (last visited 19 February 2009).
[4] *See* https://www.trustedcomputinggroup.org/home and http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html (last visited 19 February 2009).
[5] T. Kohno, et al., *Remote physical device fingerprinting*, 2 IEEE Transactions on Dependable and Secure Computing 93-108 (2005) .
[6] *See* http://urel.binghamton.edu/PressReleases/2006/Jan-Feb%2006/Fridrich.html (last visited 19 February 2009).
[7] J.D.R. Buchanan, et al., *Forgery: "Fingerprinting" documents and packaging*, 436 Nature 475 (2005) .
[8] *See* B.J. Koops and M.M. Prinsen, *Houses of Glass, Transparent Bodies: How New Technologies Affect Inviolability of the Home and Bodily Integrity in the Dutch Constitution*, 16 Information & Communications Technology Law 177-90 (2007) and EGE, *Ethical Aspects of ICT Implants in the Human Body* (European Group on Ethics in Science and New Technologies, 2005).
[9] *See, e.g.,* A. Küpper, *Location-based services: fundamentals and operation* (Chichester, England; Hoboken, NJ: John Wiley 2005); D.J. Phillips, *Texas 9-1-1: Emergency Telecommunications and the Genesis of Surveillance Infrastructure*, 29 Telecommunications Policy 843–56 (2005) ; M.S. Monmonier, *Spying with maps: surveillance technologies and the future of privacy* (Chicago: University of Chicago Press 2002), at 13: 'Equally adept at tracking vehicles, employees, adolescents, and convicted criminals, GPS is very much a surveillance technology, with credible threats to personal privacy.'

based on their location.[10] All of these developments imply that, contrary to the past, when the location of things and people was usually observed, if at all, by eye witnesses, nowadays, their location is stored and can be retrieved automatically for considerable periods without loss of memory.

Yet other examples of new types of data that are becoming available are Internet surfing data ('you are what you surf'), sensorial (tactile and perhaps olfactory) data in not-too-distant virtual reality applications, and information from DNA, including phenotypical information (e.g., hair and skin colour) and geographical background.[11]

Second, the *amount* of data – new and old types – that are generated, processed, and stored is exploding. For example, more and more street and semi-public situations routinely are captured and stored by CCTV systems, not primarily for criminal investigation purposes, but often secondarily usable as evidence in court. The boom of 'preventative picture-taking' is well illustrated by new self-service postal machines in the US, that for certain transactions make a picture of the user and store this for 30 days, so that potential senders of unpleasant post can be traced more easily.[12]

The best example of the explosion of data, however, is the Internet. A small but salient remark posted to an obscure news group in 1992 can still haunt someone decades later because the archive is online and searchable. Many a remark, joke, or blurt-out that once upon a time would only have been made in bars or across the hedge is now made and stored on the Internet, in blogs, chatrooms, and social network sites, with a level of intimacy that used to be reserved only for the closest personal friends. When now you meet someone new who greets you with a "Hi, I just googled you", the realisation of what she may have read and seen – including what others say about you – makes you feel slightly unsettled.[13] But it is not only statements and facts that are increasingly stored: web services facilitate online storage of photos, documents, spreadsheets, calendars, diaries, and what not, so that you can access them from any place at any time. This is enormously convenient, of course, but it implies that also others – like the police – can obtain from third parties intimate records that used to be stored only in the fortress of one's home. Moreover, the oddest pictures and movies are published on the Internet, not only by exhibitionists but also by fans, video artists, Nosey Parkers, and perverts like happy slappers, and you may well be among the unaware victims thus displayed to the public. In short, the Internet has created a dynamic of recording and publishing the weirdest and most intimate details in word, image, and sound, facilitated by ubiquitous and cheap recording and publishing equipment.

Another dynamic is also worth mentioning: the struggle over content and copyright. The Internet facilitates massive leaks in the content business, with a counterreaction of Digital Rights Management (DRM) systems, which enable copyright holders not only to control content, but also, as a byproduct, to gain insight in the private use of content: when, where, and how often does someone listen to a song or watch a movie? The private sphere used to be closed off from copyright enforcement, but nowadays, the content industry wants to see and investigate users' hard disks.[14] In former times, people listened to the radio without anyone knowing, but today, Internet radio precisely monitors which IP address listens when to which radio programmes.[15] Unrelated to copyright enforcement, a similar dynamic leads to storing all kinds of data in other equipment for security or convenience purposes, from cars recording how fast they drive when and where (without a safety belt but telephoning when the accident happened?!), to refrigerators storing their contents to warn the user that they should really finish the milk today and get new mayonnaise tomorrow.[16]

---

[10] D.E. Denning and P.F. MacDoran, *Location-Based Authentication: Grounding Cyberspace for Better Security*, Computer Fraud & Security 12-16 (1996) ('Geodetic location can be useful for locating the perpetrators of cyber crimes').

[11] On forensic DNA phenotyping, *see infra*, Section 4.2.

[12] *See* http://www.epic.org/privacy/postal/postalapc.pdf (last visited 19 February 2009).

[13] Google's top executive, Eric Schmidt, was apparently not amused when he was googled in a news report about Google's increasing influence (Elinor Mills, 'Google balances privacy, reach', News.com 14 July 2005), *see* Randall Stross, 'Google Anything, So Long as It's Not Google', *New York Times* 28 August 2005.

[14] Apart from the many cases of content industry asking for users' IP addresses from Internet Service Providers, perhaps the most illustrative example of this movement is Sony's rootkit, *see* http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html (last visited 19 February 2009).

[15] *See* B.J. Koops and R. Leenes, *"Code" and the Slow Erosion of Privacy*, 12 Michigan Telecommunications & Technology Law Review 115-88 (2005) at 129-132.

[16] On domotics and the implications for surveillance, *see* Koops and Prinsen, *Houses of Glass*, *supra*, note 8.

2.2 Accessibility of Data

A second relevant trend is that data become increasingly accessible. Especially the combination of digitisation and automated recognition allows for much easier access to data. Rather than having to watch 48 VHS video tapes to see whether they contain child porn, a scan of a hard disk or news group will easily recognise known child-porn pictures. Face recognition and aggression detection systems enhance the possibilities of camera surveillance, to name but two forms of pattern recognition.[17] Connecting and converging technologies do not only enable Voice over IP, but Everything over IP, so that all types of sound and image (and shortly sense and smell) can be transmitted anytime anyplace. The combination of connectivity and automated recognition has even facilitated finding hitherto unknown data: knowledge discovery in data bases. Companies like Omnitrace have emerged, which connect all sorts of public data bases in order to provide profiles or personal data to trace people.[18] The police can buy such data bases and merge them with their own data warehouses, for example, to uncover unknown criminal links in a certain sector of society. The possibilities of profiling is one of the reasons why police data bases – not only fingerprints and DNA, but also observations and personal data from daily practice – continue to grow, and are increasingly interconnectable or connected.[19]

Another aspect of growing availability is the ease with which persons can be monitored at a distance.[20] Cars can be traced when equipped by gadgets like TeleAid,[21] but also by automated number-recognition systems, for example, for road-pricing purposes. Computers can be remotely searched, for example when their WiFi access is not secured or when their network protection is breached by malware (which could be a Trojan police horse or key sniffer). Unmanned aerial vehicles easily allow taking aerial photos without being noticed. Cameras are being developed that can see through walls and clothes,[22] equally novel are 'sniffing chips', detector wasps, and olfactory sensors usable for detecting suspicious or revealing smells[23]. Compared to such new technologies, a thermal imager used in helicopters to discover hemp plants (betrayed by their heat radiation) – which the US Supreme Court found to violate the Fourth Amendment because the technology was not (yet) in general public use[24] – is a distinctly primitive technology. All this implies that the traditional boundaries of private life - clothes, walls, time, and place – dissolve, and no longer protect against Peeping Toms.

Moreover, this trend is reinforced by the miniaturisation of surveillance technologies. Directional microphones, which a few decades ago were bulky and clumsily visible when carried across the street, now fit unnoticeably into the arm of a pair of glasses. It is not always easy to see when someone makes a picture with her mobile phone, but a camera hidden in a buttonhole (very cheap nowadays in 'spy shops') is sure to allow for undetectable monitoring.

---

[17] Pattern recognition is considered by the Dutch police the 'most promising' new technology to combat crime, Commissie Criminaliteit en Technologie, *Technologie en misdaad. Kansen en bedreigingen van technologie bij de beheersing van criminaliteit* (2005), at 11. Compare RAE's vision: 'Digital surveillance means that there is no barrier to storing all footage indefinitely and ever-improving means of image-searching, in tandem with developments in face and gait-recognition technologies, allows footage to be searched for individual people. This will one day make it possible to "Google spacetime", to find the location of a specified individual at some particular time and date.' Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance. Challenges of Technological Change* (RAE, 2007), http://www.raeng.org.uk/policy/reports/pdf/dilemmas_of_privacy_and_surveillance_report.pdf (last visited 19 February 2009), at 7.

[18] http://www.omnitrace.com (last visited 19 February 2009).

[19] *Cf.* Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM(2005) 597final.

[20] *See*, generally, Monmonier, *supra* note 9, and J.K. Petersen, *Understanding surveillance technologies: spy devices, their origins & applications* (Boca Raton, FL: CRC Press 2001).

[21] TeleAid allows a service centre to listen to what happens in a car; it can be used, eg, to track a hi-jacked car with two infants on the back seat ('Carjacked but Tracked. High-Tech System Helps End Chase Of Stolen SUV Carrying 2 Toddlers', *Washington Post* 17 July 2003).

[22] *See, e.g.,* the body scanner used in a pilot project at Heathrow Airport in 2004 and at Schiphol Airport in 2007; the Heathrow project was stopped when shocked passengers found out they were seen in the nude by the scanner ('Plane passengers shocked by their x-ray scans', *Sunday Times* 7 November 2004).

[23] Crime Prevention Panel, *Just Around the Corner. A consultation document* (DTI, 2000), http://www.foresight.gov.uk/Previous_Rounds/Foresight_1999__2002/Crime_Prevention/Reports/Just%20Around%20the%20Corner/CrimeConsultation.pdf (last visited 19 February 2009), at 12-13.

[24] *Kyllo* v *United States*, 533 U.S. 27 (2001), 121 S.Ct. 2038, 150 L.Ed.2d 94.

The 'smart dust' scenario is approaching, in which dust particles equipped with a sensor and transmitter are spread to monitor an area or a person.[25]

Taken together, these developments enhancing availability cause the police to have a wide range of technologies available to collect, connect, and store ever more data, without this being known to the persons being monitored.

There is also an opposite trend, however: data can increasingly be better protected, thus lessening their accessibility. The classic technology for this is cryptography. Contrary to traditional ciphers, modern cryptography, at least when used correctly, is uncrackable. In the 1990s, many a government feared that criminals would become uncatchable by using encryption;[26] this has not proved true, even if since two or three years, law enforcement encounter somewhat more encryption in daily practice. It is unknown to what extent steganography – methods to hide data in innocuous-looking pictures or files – is used (after all, it is invisible when used correctly!), but it is not likely to be widely applied.[27] A more important shielding technology is the use of crypo-enabled computer networks, such as Freenet for 'file swarming' (storing a file cut in bits and pieces across the world, only accessible with the right user name and password), or Tor for unlinkable communications (bouncing messages across a global network, making traffic analysis impossible). Cryptography also features in many Voice over IP applications, such as Skype, so that intercepted communications cannot be read. Intercepting communications also becomes more difficult for other reasons, like the use of small, decentralised networks, seamless roaming, and an explosion of telecommunications protocols.[28] Altogether, the rise of 'disconnection technologies' (technologies that provide access control to services and resources, to maintain the security of data)[29] implies that, at least in theory, law enforcement agencies can only access data by requesting or forcing end users to provide them with the relevant password or the data themselves. This is a questionable approach since the privilege against self-incrimination may imply that data and even passwords cannot legally be ordered from suspects.[30] However, in practice, law enforcement seems rarely completely blocked because of shielding technologies applied by criminals; often, the technologies are applied carelessly (eg, writing down a password), or alternative investigation measures yield sufficient evidence.[31]

If we put together the technological trends of increasing amounts and availability of data with the trend of better protection of data, we may well conclude that the former by far outweigh the latter. As the UK Royal Academy of Engineering notes, 'while connection is easy disconnection is difficult. That is to say, it is relatively simple to create a network between a set of computers, but it is difficult to partition the data on a computer within a network so that

[25] *See* http://robotics.eecs.berkeley.edu/~pister/SmartDust/ (last visited 19 February 2009). Crime Prevention Panel, *supra*, note 23, at 16 expects that '[m]iniaturisation has potentially significant implications for crime detection'.

[26] *See, e.g.,* L.J. Hoffman (ed.) *Building in Big Brother. The Cryptographic Policy Debate* (New York: Springer 1995) and B.J. Koops, *The Crypto Controversy. A Key Conflict in the Information Society* (The Hague etc.: Kluwer Law International 1999).

[27] An interesting case of steganography, however, is the Dutch 'sweet terrorist' who extorted dessert producer Campina: he asked data he needed to acquire the ransom to be hidden in a photograph of a car, to be placed on a large car website. He was caught because he searched for the photo immediately after it was placed, and the American anonymisation service that he was using voluntarily provided his IP address to the Dutch police. Hof [Court of Appeal] Amsterdam 30 November 2004, LJN AR6799, www.rechtspraak.nl. For an account (in Dutch) of the investigation process, *see* http://www.netkwesties.nl/editie67/artikel1.php (last visited 19 February 2009).

[28] *See* B.J. Koops and R. Bekkers, *Interceptability of telecommunications: Is US and Dutch law prepared for the future?*, 31 Telecommunications Policy 45-67 (2007) .

[29] Royal Academy of Engineering, *supra*, note 17, at 14.

[30] See, in particular, ECtHR 3 May 2001, *J.B.* v *Switzerland*, Appl. No 31827/96; District Court Vermont, *United States* v *Boucher*, 2007 WL 4246473 (29 November 2007).

[31] The use of (effective) shielding technologies by criminals is largely restricted to large international, organised groups. The Dutch police (Dienst Nationale Recherche Informatie, *Nationaal dreigingsbeeld zware of georganiseerde criminaliteit. Een eerste proeve* (KLPD, 2004), http://www.politie.nl/KLPD/Images/35_87797.pdf, at 44) noted that with the exception of such groups, 'shielding technologies are often applied in a sloppy way' by criminals, allowing the police to access data nonetheless. Also significant is the finding in the US wiretap reports that no encryption was encountered during any federal or state wiretap (Administrative Office of the United States Courts, *2007 Wiretap Report* (U.S. Courts, 2008), http://www.uscourts.gov/wiretap07/contents.html (last visited 19 February 2009)).

the data can only be accessed by certain computers or users.'[32] In the on-going process of hide and seek between criminals and law enforcement, seeking data is facilitated much more by current technological trends than hiding data.

3 Social Context

3.1 Risk Aversion and the Culture of Control

Since 1986 when Ulrich Beck coined the term, current society has evolved more and more into a 'risk society', a paradigmatic shift from the classic industrial society occupied with distributing wealth to a late-modern industrial society occupied with distributing risks. The key question is:

> How can the risks and hazards systematically produced as part of modernization be prevented, minimized, dramatized, or channelled? (…) Questions of the development and employment of technologies (in the realms of nature, society and the personality) are being eclipsed by questions of the political and economic "management" of the risks of actually or potentially utilized technologies.[33]

Where Beck mainly centred his argument on environmental risks and hazards, risk discourse can nowadays be found in debates ranging from genetic engineering, privacy and identity, to immigration, domestic violence, and social divides.[34] As a result, problems are often phrased in terms of 'risk management', and 'risk governance' has risen as a new academic discipline.[35]

Along with risk as a keyword in public and political debates, society increasingly seems to tend towards risk aversion. Although most people would rationally agree that ultimately, not all risks can be eliminated, not even if unlimited resources were available, newspapers and parliamentary debates tend to blow up accidents, disasters, and attacks and consequently demand all possible action to prevent similar harm from happening in the future.[36] A relatively small number of high-profile incidents – most visibly some terrorist or political crimes (the September 11 attacks, the London terrorist attacks, the murders in the Netherlands of politician Pim Fortuyn and film director Theo van Gogh), but also incidents with, for example, young victims (like the 'Maasmeisje' and 'Savannah' in the Netherlands, Megan Kanka in the US, and James Bulger in the UK) – dominate public and political debate for years and trigger policies and legislation designed to generically prevent future repetitions. Through risk aversion, society tends to transform itself into a 'safety state' in which safety – the real or perceived absence of danger – is an overarching value that trumps all other considerations.[37]

Framing social developments in terms of risk and desiring to eliminate danger as much as possible almost logically lead to a culture of control. David Garland has most powerfully analysed this trend in the context of crime control and penal climate, for both the United Kingdom and the United States.[38] The Netherlands used to be known as having a much more liberal, tolerant culture in terms of crime control, but since a decade or so, it seems well on its way to acquiring a similar culture of control.[39] This culture is a wider trend than crime control, however:

---

[32] Royal Academy of Engineering, *supra*, note 17, at 4.
[33] U. Beck, *Risk society: towards a new modernity* (London ; Newbury Park, Calif.: Sage Publications 1992), at 19.
[34] *Cf.* B. Adam, et al., *The risk society and beyond: critical issues for social theory* (London; Thousand Oaks, Calif.: SAGE 2000); R.V. Ericson, *Crime in an insecure world* (Cambridge, UK; Malden, MA: Polity 2007).
[35] *See* M.B.A.v. Asselt, *Risk governance: Over omgaan met onzekerheid en mogelijke toekomsten* (Maastricht, 2007).
[36] *Cf.* Garland, *supra*, note 2, at 192: 'The prevailing attitude is that it is better to keep a known criminal locked up for ever than to risk the life or property of another innocent victim.' For the Dutch situation, *see* H. Boutellier, *De veiligheidsutopie: hedendaags onbehagen en verlangen rond misdaad en straf* (Den Haag: Boom Juridische Uitgevers 2002) and N.J.H. Huls, *Recht in de risicomaatschappij* (Delft, Delft UP, 1997).
[37] *See* C. Raab, *The Safety State*, inaugural lecture Edinburgh (unpublished, 2004).
[38] Garland, *supra* note 2.
[39] Whether or not the Netherlands have a culture of control (yet) has not been mapped in as much detail, but there is an evident trend towards a harsher penal climate. *See* G.A.A.J. Van den Heuvel, *Reflecties over actueel risicostrafrecht*, in Veiligheid of vergelding? Een bezinning over de aard en functie van het strafrecht in de postmoderne risicomaatschappij, 79-92 (Deventer: Kluwer, E. Prakken ed., 2003), Vedder, et al., *supra* note 2, and particularly Cavadino and Dignan, *supra* note 2, at 113-128 and D. Downes and R. Van Swaaningen, *'The Road to Dystopia? Changes in the Penal Climate of the Netherlands'*, in Crime and Justice in the Netherlands, 31-71 (Chicago; London: University of Chicago Press, C. Bijleveld ed., 2007) at 66: 'Dutch exceptionalism as a

> Spatial controls, situation controls, managerial controls, system controls, social controls, self-controls – in one social realm after another, we now find the imposition of more intensive regimes of regulation, inspection and control and, in the process, our civic culture becomes increasingly less tolerant and inclusive, increasingly less capable of trust.[40]

Although it is not prominent in Garland's analysis, technology is a key enabling factor in the move towards the culture of control: the economic risk calculus associated with this culture depends on ICT, just like the channelling of space and people for enhanced control would not be possible without the designing, profiling, and classifying power of modern computing.

3.2 Surveillance Society

Closely related to the emering risk society is the expansion of surveillance technologies and infrastructures. The development of risk aversion and the culture of control, with technological developments (see 'Techological Context' above) as a key enabling factor, is inextricably linked to the rise of the surveillance society. This has been most convincingly demonstrated by David Lyon's analysis of technological and social developments since the 1960s that culminate in late modern society's 'monitoring everyday life in a constantly expanding range of contexts'.[41]

Surveillance nearly always, albeit in different ratios depending on the context, has two faces: care and control. The fact that often the element of care is stressed by those in power who implement surveillance infrastructures – this technology watches over you and contributes to your and society's safety – partly explains why the surveillance society has developed so quickly over the past two decades or so.[42] The control face of the enormously prevalent CCTV in the UK, for example, is easily outweighed by its care face of 'solving' high-profile cases of James Bulger (1993) and the 7/7 London transport attacks (2005). Potential negative aspects of CCTV, including the sometimes doubtful evidence whether it really enhances safety, are downplayed because of the risk society's need for uncertainty reduction. Another reason why surveillance is often accepted so easily is that it is usually contrasted only with privacy, which – at least until very recently, the tide may be slowly turning since one or two years – had little political value in policy decisions in US, the UK, and the Netherlands. Moreover, by framing privacy as an individual need (especially through the concept of informational self-determination, which is as overrated in academic literature as it is underrated in policy and practice), the social dimension of privacy as a collective need of the democratic constitutional state is neglected. Also, other downsides of surveillance, such as inequality through profiling and social sorting, are neglected in policy-making.[43] The result is that surveillance benefits those already in control, making the strong even stronger, while relatively few measures are taken to serve as countervailing powers.

The surveillance society is much broader than a society steeped in criminal investigation and intelligence monitoring of citizens. Much 'routine, mundane surveillance (...) is embedded in every aspect of life',[44] including private-sector monitoring of work, health, and consumer

---

relative penal utopia no longer exists. Despite all the differences in time, size, and intensity, the Netherlands is following much the same lines as David Garland [analyzes] for the United States and England'.

[40] Garland, *supra* note 2, at 194-195.

[41] D. Lyon, *Surveillance society: monitoring everyday life* (Buckingham England ; Philadelphia: Open University Press 2001), at 133. *See* also D. Lyon, *The electronic eye: the rise of surveillance society* (Minneapolis: University of Minnesota Press 1994); D. Lyon, *Theorizing surveillance: the panopticon and beyond* (Cullompton, Devon: Willan Publishing 2006); House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State* 2009), http://www.parliament.the-stationery-office.com/pa/ld/ldconst.htm. For examples how everyday life is monitored in the surveilllance society of 2006 and of 2016, *see* D. Murakami Wood (Ed.), *A Report on the Surveillance Society. For the Information Commissioner by the Surveillance Studies Network* 2006), http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf (last visited 19 February 2009), at 48-75. Surely, these studies cannot be accused of 'crude characterisations of our society as a surveillance society in which all collections and means of collecting information about citizens are networked and centralised in the service of the state' that the House of Commons Home Affairs Committee, *A Surveillance Society?* (House of Commons, 2008), at §14, rejects. The analysis of Lyon and others stresses how surveillance, far from being centralised in the service of the state, is daily practice of many actors in many ways.

[42] *Cf.* Lyon, *Surveillance Society* , *id.*, at 3 and 136-137.

[43] *Cf. id.* at 128-137; M. Hildebrandt and S. Gutwirth (eds), *Profiling the European Citizen. Cross-disciplinary perspectives* Springer 2008).

[44] Lyon, *Surveillance Society* , *id.*, at 1. Lyon has updated and further substantiated this analysis in Lyon, *Theorizing Surveillance*, *supra* note 41, at 1: 'Surveillance has become ubiquitous and taken for granted in today's world'.

preferences. Although we are constantly being monitored in some way or another, we do not live in an Orwellian 'Big Brother' dystopia: the surveillance is too fragmented across infrastructures and information flows for a single authority to know everything about everyone. Rather, an intricate network of small surveillance societies exists, often overlapping, connectable, or connected, but each with their own features and rules.

3.3 Politicised Criminal Law

The third, again related, social trend that is relevant to my argument is that criminal law and criminal policy have become increasingly politicised over the years. Although the shaping of criminal law and policy has always had a political besides a legal dimension, politics increasingly trumps considerations based on criminal law principles.[45] Without going into complex questions of the interrelationship between law and politics, it can be observed that legal measures are often motivated by political arguments, with politicians feeding the media with tough-on-crime statements, public polls calling for more security, media enlargement of security incidents, and politicians' desires to show they meet the public's demands by increased security measures. A relevant illustration is the UK House of Lords Home Affairs Committee, who explain the rise of surveillance partly by 'the public's need' for increased criminal investigation: 'We also accept that advances in technology have heightened the public's expectations of what technology can deliver not only in terms of convenience but also in connection with the prevention and investigation of crime'.[46] This suggests that legal measures for preventing and investigating crime respond to public expectations and perceptions of insecurity rather than intrinsic needs of crime-fighting and actual insecurity. Boundaries set by the legal system of checks and balances are crossed because a political need is felt to show that the *vox populi* – and the public have become increasingly vociferous in the age of Web 2.0 – is listened to.

It is impossible to determine what is cause and effect here, since politics, media, and public perception mutually reinforce each other. But whatever the initial trigger, in this arena, the dog of politics keeps chasing its voters' and media tail and can hardly stand still to listen to legal-systematic or empirical legal arguments that are often too subtle, too much framed in alien jargon, or based on unfamiliar theoretical assumptions, to be able to penetrate public or political debate. This is not to say that legislation has become completely politicised – in certain areas, legal reasoning does inform the political debate[47] – but at least in the sphere of public security and crime control, the spheres of political and legal-academic debate seem increasingly to be growing apart.[48] One important consequence of this is that criminal law tends to develop relatively independently from basic tenets of criminal legal doctrine, which, through multiple individual developments, may incrementally lead to a paradigm shift in criminal law.

4 Developments in Criminal Law

The technological and socio-political trends sketched so far are key factors in the changes that are taking place in criminal law. In this section, I will demonstrate how the footprint of criminal law is becoming larger and larger, through expanding substantive and procedural criminal law and changes in society's architecture for crime-prevention purposes. The contours are visible of a 'crime society': a society where criminal law is a primary form of social control. As Jonathan Simon observes, 'it is not just the scope of this wave of lawmaking

[45] N. Lacey, *The prisoners' dilemma: political economy and punishment in contemporary democracies* (Cambridge, UK; New York: Cambridge University Press 2008), at 22: 'crime became an increasingly politicised issue, and the era of "penal populism" was born', and at 101-02: in 'societies such as Britain and the USA, (…) it comes naturally to think of law as the tool of policy rather than as an autonomous system whose doctrinal standards place constraints on power'; A. Ashworth, *Principles of criminal law* (Oxford; New York: Oxford University Press 2006), at 52: 'The main determinants of criminalization continue to be political opportunism and power, both linked to the prevailing political culture of the country.'

[46] House of Commons Home Affairs Committee, *supra* note 41, at §77.

[47] Ashworth, *supra* note 45, at 25.

[48] *Cf.* A. Ashworth, *Is the criminal law a lost cause?*, 116 Law Quarterly Review 225-56 (2000) who, at 225, mentions the 'unprincipled and chaotic construction of the criminal law', in which '[p]oliticians, pressure groups, journalists and others often express themselves as if the creation of a new criminal offence is the natural, or the only appropriate, response to a particular event or series of events giving rise to social concern.' For a Dutch example in the anti-terrorism area, *see* the analysis of M.J. Borgers, *De vlucht naar voren*, (Den Haag, Boom Juridische uitgevers, 2007).

that makes it impressive, it is also the coherence of this body of law as reflecting a vision of how institutions govern through crime.'[49]

The role of technology in this process is important to highlight for two reasons. First, technology often plays a facilitating role. I shall illustrate each aspect of the emerging crime society with examples from technology regulation; for each aspect, other examples exist, but the technology-related ones are as exemplary as any, and particularly for the aspects of expanding policing and changing architecture, they should be considered as predominant. Second, even though the increasing footprint of criminal law often also has other *causes* than technology, the *effects* of technology have to be taken into account. Today's large-scale collection, processing, and storage of data for criminal-law purposes imply a significant qualitative difference with policing practices of the past, for example of the 1950s and 1960s. Rather than relying on police *officers* to recognise people and patterns and to remember criminal acts, present-day policing relies on police *technology* (like computers and sensors) to recognise people and patterns and to remember the past; and contrary to people, computers have accurate, unrelenting, and virtually unlimited memories. This has vast implications for legal protection as we gradually move towards large-scale monitoring of citizens and more preventative approaches.

4.1 Expanding Substantive Criminal Law

More and more forms of human behaviour are being criminalised, in which technology often plays an important facilitating role. An increasing footprint of substantive criminal law can, for example, be seen in the area of cybercrime, where criminal liability expands both in time – in the pre-crime stage of preparatory acts – and in scope – with new, 'virtual', activities being criminalised.[50] Many other examples can be given of other types of ICT-related activities that are increasingly criminalised.[51]

However, technology's facilitating role is broader, and more subtle, than that. Because technology tends to enable discovering information much more than hiding it, technology is a crucial factor in the explosion of regulatory laws that seek to control more and more areas of life. '[I]nnovative surveillance technologies and networks (…) all facilitate criminalization of the merely suspicious and of security failures.'[52] The majority of the new criminalisations in the UK, as evidenced for example by Ashworth's analysis of a sample year, 1997, concern regulatory offences, enforced by administrative authorities,[53] and the UK nor 1997 are exceptional in this respect. This type of regulation would simply not be possible without the efficient, large-scale data creation, storage, and processing that the advent of computers has enabled since the 1980s. Similarly, the increasing peering into people's private files to uncover copyright infringement, and a parallel increasing criminalisation of copyright infringements, is not only caused by the rise in copyright infringements caused by peer-to-peer systems, but equally by the fact that the very same ICT enables detailed monitoring of what each and every individual does at home.[54]

In a similar vein, the measure of Anti-Social Behaviour Orders (ASBOs) allows authorities in the UK to impose an injunction on someone to refrain from further 'anti-social' behaviour, a breach of which is a criminal offence. This has brought a whole array of forms of behaviour, which previously would have been considered merely odd or uncivilised, into the realm of

[49] Simon, *supra* note 2, at 75.
[50] *See* the Convention on Cybercrime, CETS 185, which has been ratified by the Netherlands and the United States, but not yet by the United Kingdom. Article 6 criminalises preparatory acts or, in the convention's terminology, 'misuse of devices', such as possessing a password with which a computer can be illegally accessed, if the possessor has the intent to use it for committing a cybercrime. Article 9(2)(c) criminalises virtual child pornography, ie unreal images that look like real images, depicting minors in a sexual context.
[51] See, for example, the criminalisation of grooming, in Art. 15 of the UK Sexual Offences Act 2003 and Art. 23 of the Lanzarote Convention, CETS 201; prohibiting sex with animals and animal porn, including 'virtual animal porn', in the Dutch Prohibiting Sex with Animals Bill, *Kamerstukken I* [Parliamentary Documents First Chamber] 2007/08, 31 009, A; and the UK House of Commons' call that '[t]ougher penalties for negligent information-handling should be introduced in order to make clear where the burden of responsibility lies', House of Commons Home Affairs Committee, *supra* note 41, at 61.
[52] Ericson, *supra* note 34, at 2.
[53] Ashworth, *Lost cause*, *supra* note 48, at 227-228.
[54] *Cf.* S. Penney, *Crime, Copyright, and the Digital Age*, in What Is a Crime? Criminal Conduct in Contemporary Society (UBC Press, Law Commission of Canada ed., 2004).

criminal liability.[55] Like with regulatory offences, the practice of ASBOs is facilitated through the surveillance capabilities that modern technologies like cameras and computer data bases bring. Hence, the emerging shadow of criminalisation of 'anti-social' behaviour has been significantly facilitated by technology. In a somewhat similar development, school discipline in the United States has been stepped up in recent years, with the adoption of 'practices suggestive of the penal aspects of criminal justice'.[56] The environment shaped by the Safe Schools Act[57] has led to relatively mundane policies like those concerning school uniforms to be monitored and used, facilitated by software, in terms reminiscent of crime statistics, as evidenced by the following example:

> Using U.S. Department of Education software to track discipline data, Ruffner has noted improvements in students' behavior. Leaving class without permission is down 47 percent, throwing objects is down 68 percent and fighting has decreased by 38 percent. Staff attribute these changes in part to the uniform code.[58]

In general, the culture of control that is visible from the rise of administrative and anti-social behaviour regulation, reinforced by criminal provisions, as well as by non-governmental disciplining initiatives of governing through crime, relies heavily on the data infrastructures resulting from the rise of computers over the past decades, that now form the core of the information society. Likewise, the culture of control's shift in attention from pathological, abnormal offenders to mundane, opportunist offenders[59] is made possible by the rise of the technology-pervaded surveillance society that closely monitors everyday life. As a result, building on the pillars of the information society, substantive criminal law no longer only covers extreme or particularly damaging forms of behaviour, but it has moved its tentacles into all spheres of social life, as just any other – but potentially extremely powerful – mode of social control.[60]

4.2 Expanding Procedural Criminal Law

Criminal-investigation powers have increased significantly over the past two or three decades. Although one could be tempted to think that 9/11 was a watershed, steady expansion has taken place from the 1980s or the early 1990s onwards.[61] I will describe three key areas to illustrate this.

Interception of communications has expanded greatly in the US and, particularly, in the Netherlands.[62] In the United States, interception of phone ('wire') communications was regulated after *Katz* interpreted the Fourth Amendment to protect telephone communications.[63] In 1986, the Electronic Communications and Privacy Act enabled the interception of electronic communications, under less strict conditions than for wire interception, allowed wiretapping for more types of crimes, and introduced 'roving' interception (following the suspect to be intercepted rather than fixed lines or places).[64] The Patriot Act of 2001 again allowed interception for more crimes, and it transferred voice mail from the wiretap regime to the less protected communications storage regime.[65] The Netherlands saw a largely similar development of expansion.[66] Particularly significant was the broadening of the scope of interception, enacted in 2000 in the Special Investigation Powers

---

[55] *See* s 1 et seq Crime and Disorder Act 1998, as amended several times since 1998. For a critical discussion of ASBOs, *see, e.g.,* S. Macdonald, *A Suicidal Woman, Roaming Pigs and a Noisy Trampolinist: Refining theASBO's Definition of "Anti-Social Behaviour"*, 69 Modern Law Review 183-213 (2006) .
[56] Simon, *supra* note 2 at 221.
[57] Public Law 103-227, 31 March 1994, 108 Stat. 200, et seq., 20 U.S.C.A sect. 5960 et seq.
[58] Simon, *supra* note 2 at 225.
[59] Garland, *supra* note 2, at 187.
[60] Simon, *supra* note 2; Ericson, *supra* note 34.
[61] *See, e.g.,* Garland, *supra* note 2; the yearly Privacy and Human Rights reports by EPIC and Privacy International; Lyon, *The electronic eye* and Lyon, *Surveillance Society* , *supra* note 41; S. Garfinkel, *Database Nation. The death of privacy in the 21st century* (Cambridge: O'Reilly 1999); House of Commons Home Affairs Committee, *supra* note 41, Vedder, et al., *supra* note 2.
[62] In the UK, it has evolved less dynamically (or less visibly), largely because interception can only be used for intelligence and not for evidence purposes.
[63] *Katz* v *United States*, 389 U.S. 347 (1967); Title III, Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §2510 et seq.
[64] Pub. L. 99-508, 21 October 1986, 100 Stat. 1848.
[65] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56, 26 October 2001.
[66] A.H.H. Smits, *Strafvorderlijk onderzoek van telecommunicatie* (Nijmegen, Wolf Legal Publishers, 2006).

Act (Wet bijzondere opsporingsbevoegdheden), to allow interception of the connection not only of suspects but also of non-suspects, provided such interception could further the investigation.

While the law in the books has thus been broadened over time, an equally important expansion of interception can be observed in law in practice. In the US, the number of interception orders (for criminal investigation, not for intelligence or national security) has more than tripled since 1987 (from 673 to 2208 in 2007), and the average number of intercepted communications in each case has more than doubled (from 1299 to 3106 in 2007), so that the total amount of communications intercepted has almost octupled.[67] In the Netherlands, the figures (as far as they are available, since they were not registered or published officially until 2008) are much higher: in 1993, 3619 interception authorisations were granted for criminal investigation (more – in absolute terms – than in the US: the Netherlands is truly a wiretap nation),[68] rising through 10,000 in 1999 to some 25,000 authorisations in 2007.[69] This does not mean that over a decade, 10 times more people have been under wiretap, because authorisations are given for separate connections such as fixed phones and mobile phones (and criminals have substantially more phones nowadays), but the trend is undeniably upwards. One should also note that given the enormous increase in communications at large, particularly since the advent of mobile phones (including sms) and the Internet, perhaps the percentage of all communications intercepted may actually have decreased, but in absolute figures, many more data have become available to the police through intercepts. And this is not only a quantitative increase, but also a qualitative increase, given the technological trend of new types of data (such as Internet browsing and location data) that allow long-distance glimpses of human life that were previously hidden to the police, or observable only against significant effort and costs.

The second example is DNA forensics, where a similar development can be observed. Since the invention of DNA fingerprinting in the 1980s, investigation powers in DNA forensics have gradually expanded.[70] In England and Wales, the power to take DNA samples, introduced by the Police and Criminal Evidence Act 1984, was extended in 1994 and 1996. In 2001, the Criminal Justice and Police Act allowed the retention of samples even if people were not prosecuted or convicted of a recordable offence.[71] In the Netherlands, taking a DNA sample from a suspect was allowed for more types of crime and without a magistrate's warrant in 2001, and a 2004 law allowed the Public Prosecutor to take samples from convicts in order to deter them from committing new crimes and to ensure more future matches with repeat offenders.[72] The UK database, NDNAD, has expanded enormously over the past decade, up to 4 million profiles in 2007 (around 6% of the UK population), with routine sampling and profile retention from arrestees for all kinds of crimes but also from victims and consenting witnesses and volunteers.[73] Although it is not (yet) the stated intention, UK practice carries the impression of effectively using a growth model that evolves towards a nation-wide DNA database. The US national database, CODIS, is smaller in scale, but has recently outgrown the UK database, with 4.6 million person profiles in 2007 (around 1.5% of the population).[74] The Dutch database is more restricted, but has nevertheless exploded

[67] Data retrieved from the 1997 (which includes 1987 data) and 2006 annual Wiretap Reports of the Administrative Office of the US Courts, http://www.uscourts.gov/library/wiretap.html (last visited 19 February 2009).
[68] At least in terms of criminal investigation. Wiretapping for intelligence purposes may yield a quite different picture, although it is difficult to compare these due to the official secrecy associated with intelligence practice.
[69] The 1993 figure is from Z. Reijne, *Tappen in Nederland* (WODC / Gouda Quint 1996). The 2000 figure is mentioned in Parliamentary Documents Second Chamber (*Kamerstukken II*) 2000-01, 27 591, No. 2. The 2007 figure is my extrapolation of the 12,491 authorisations granted in the second half of 2007, as mentioned in Parliamentary Documents Second Chamber (*Kamerstukken II*) 2007-08, 30 517, No. 6 – the first systematic Dutch wiretap figures to be officially published.
[70] R. Williams, et al., *Genetic Information & Crime Investigation. Social, Ethical and Public Policy Aspects of the Establishment, Expansion and Police Use of the National DNA Database* 2004); Nuffield Council on Bioethics, *The forensic use of bioinformation: ethical issues* (London: Nuffield Council on Bioethics 2007) at 3 and 9; M. Prinsen, *Forensisch DNA-onderzoek. Een balans tussen opsporing en fundamentele rechten* (Nijmegen, Wolf Legal Publishers, 2008).
[71] The current English and Welsh practice of retaining profiles and samples from unconvicted offenders should be changed, however, in light of the European Court of Human Rights' judgement in *S. and Marper* v *United Kingdom*, 4 December 2008, Nos 30562/04 and 30566/04.
[72] Act of 5 July 2001, *Staatsblad* [Dutch Official Journal] 2001, 335; Act of 16 September 2004, *Staatsblad* 2004, 465.
[73] Nuffield Council on Bioethics, *supra* note 70, at 9.
[74] *Id.* at 9.

since the 2004 Act, from 6,000 person profiles in early 2005, through 45,000 in December 2007, to almost 73,000 (around 0.44% of the population) in December 2008.[75]

Like in the interception example, DNA forensics has not only expanded in legislation and in quantity, but also in kind. A relatively recent development is forensic DNA phenotyping: deriving personal characteristics from crime-scene DNA in order to trace unknown suspects (e.g., by limiting the pool of possible suspects so that a dragnet investigation can be performed).[76] In England and Wales, the Forensic Science Service claims it can determine the rough geographical ancestry of the DNA sample donor,[77] and it will check for red hair and light skin pigment.[78] As genetic knowledge advances, other phenotypical characteristics, such as hair form or height, may come available. In the common law system, such use of a new technology is allowed until legislation or case-law dictate otherwise. This means that DNA can be used for phenotyping in England and Wales and in almost all US states.[79] In civil law systems, new investigation techniques can usually only be used when legislation specifically allows it. The Netherlands enacted a law to that effect, allowing phenotyping for geographic ancestry and gender; other features, like hair colour, will have to be designated by an Order in Council before the police can derive them.[80]

The third, perhaps most drastic, example are the powers to order delivery of data from third parties. In the US, these have been very broad ever since the Supreme Court's post-*Katz* adoption of the 'secrecy paradigm'[81] as the focus of the Fourth Amendment's privacy protection.[82] This implies that there is no reasonable expectation of privacy in data held by third parties, since they have been revealed to others and hence are no longer secret. As a result, such records can be ordered without Fourth Amendment protective standards like a warrant or probable cause. With the emergence of computerised data bases at the end of the twentieth century, this turns out a doctrine posing 'one of the most significant threats to privacy of our times'.[83] The effects of the doctrine are somewhat alleviated by statutory protection regulating law-enforcement access to third-party data, but the legislation is piecemeal (only covering particular third parties) and often contains lower standards.[84] As a result, 'the role of the judge in the process is diminished to nothing more than a decorative seal of approval', and 'there are many circumstances when [not even] court orders nor subpoenas are required'.[85] It is therefore possible and often altogether easy for law enforcement agencies, with only minor exceptions, to order delivery of any data that are stored with a third party somewhere.

In the Netherlands, third-party records were until recently much more protected: they could only be ordered in criminal investigations if there was an authorisation from the investigating judge, probable cause, and a clear link between the requested data and the crime or suspect. The powers to request third-party records were, however, dramatically expanded in 2006, when the Data Delivery Powers Act (*Wet bevoegdheden vorderen gegevens*) came into

---

[75] Figures published on http://www.dnasporen.nl. *See* also the comparison of UK and Dutch developments in Prinsen, *supra* note 70.

[76] *See* for a technical and regulatory discussion, B.J. Koops and M.H.M. Schellekens, *Forensic DNA Phenotyping: Regulatory Issues*, 9 Columbia Science and Technology Law Review 158-202 (2008) .

[77] This is contested, since individuals' DNA shows more variation than the variations of geographic groups of people, and because race is a social rather than a genetic concept; *see*, for example, Nuffield Council on Bioethics, *supra* note 70, at 80-81.

[78] Forensic Science Service, *Fact Sheet. Commonplace Characteristics* (2004).

[79] Only Indiana, Rhode Island, and Wyoming have outlawed forensic phenotyping; *see* Koops and Schellekens, *Forensic DNA Phenotyping*, *supra* note 76, and M. Hibbert, *DNA Databanks: Law enforcement's greatest surveillance tool?*, 34 Wake Forest Law Review 767-825 (1999) at 791-92.

[80] Act of 8 May 2003, *Staatsblad* 2003, 201.

[81] D.J. Solove, *The digital person: technology and privacy in the information age* (New York: New York University Press 2004), at 200.

[82] *United States* v *Miller*, 425 U.S. 435 (1976).

[83] Solove, *supra* note 81, at 202. Contra, O.S. Kerr, *The Case for the Third-Party Doctrine*, 107 Michigan Law Review 561-601 (2009) at 595, describing various 'doctrines [that] limit considerably the threat that the third-party doctrine poses to civil liberties.'

[84] Solove, *supra* note 81, at 202-209.

[85] *Id.* at 209. Orin Kerr describes other regulatory instruments that protect third-party records, such as mechanisms preventing abuse by secret agents, privileges for non-disclosure, and self-regulation by third parties; however, as Kerr himself points out, most of these 'are designed to deter bad faith investigations rather than to keep the government from accessing information altogether' and they 'deter wrongful abuse while permitting legitimate investigations' (Kerr, *supra* note 83, at 590-91). His analysis is therefore consistent with my main argument here that law enforcement has powers that allow them, under more or less stringent circumstances, to legitimately access any data stored in data bases somewhere.

effect.[86] The police can order delivery of all kinds of data, also about non-suspects, with an order from the public prosecutor, and identifying data even without such an order; only for sensitive data (like race, religion, health, or sexual life) is authorisation from the investigating judge required. This is still a more stringent and comprehensive legal regime than what applies in the US, but the result is much the same: any type of data can be requested from any third party, including sensitive data if a judge considers them sufficiently relevant to investigate a serious crime. This is particularly important when seen in combination with the technological development of the increase in data (section 'Technological Context above): now that almost every human activity leaves traces in data bases somewhere, a very penetrating picture of someone can be drawn by collecting data from third-party data bases.

Interception, DNA forensics and data delivery are not only illustrative in their expansion over recent decades, but also in the scope that criminal investigation nowadays has. Any aspect of life, including the most private areas of home and body,[87] can now, in principle, be searched. Surfing the wave of the culture of control, technology is the major driving force in the expansion of criminal investigation, with the political debate usually following two lines of argument. Where technology opens up new areas – to create more or new types of data – the police should be (en)able(d) to use this technology; otherwise, the criminals would have an undesirable advantage. In contrast, where technology shuts down areas – by new hiding techniques – the police should be given compensating other powers; otherwise, the criminals would have an undesirable advantage. All technological trends, in today's politicised legislative debates, thus stimulate the expansion of police powers.

4.3 Preventative Strategies and Changing Architectures

Although criminal law in the early modern days also had a focus on collective prevention, generally, it has been a reactive instrument over the past centuries.[88] Of course, criminalisation and prosecuting and imprisoning people also have a preventative goal, but the thrust of criminal law, in the traditional paradigm, is that a crime is committed before the apparatus of criminal law comes into action. Policing and the criminal-justice system have been reactive in nature.

The ability of technology to open up and connect new and ever larger streams of data, however, are partly responsible for the increasing focus within the practice of criminal law towards prevention. Illustrative – also for the development in US and UK policing[89] – is the strategic vision of 'information-led investigation' as articulated by the Dutch Council of Chiefs of Police: 'the new style of knowing and being known'. The enhanced freedom of citizens in the information society, and the consequent decrease in the government's power to react, warrant, in the police chiefs' view, a move towards monitoring and controlling 'streams', ie infrastructures and information flows. This is not merely seen as information-led investigation, but even as information-guided 'police care' (*informatiegestuurde politiezorg*). The characteristics of the new 'police care' are worth quoting in detail:

> 1. Information-guided police care goes beyond traditional boundaries like distance (GPS, integral information systems, and advanced interception techniques), darkness (ultraviolet light for night vision), and physical barriers (sensors that detect the presence of gas, explosives, weapons, drugs, and nuclear material through container walls and or other packaging materials).
>
> 2. Information-guided police care goes beyond traditional time barriers. Information is stored on a routine basis, it can be retrieved from the past, and it is combined, analyzed, and exchanged within the criminal justice system.

[86] Act of 16 July 2005, *Staatsblad* 2005, 390.
[87] *Cf.* Koops and Prinsen, *Houses of Glass*, *supra* note 8.
[88] *Cf.* Garland, *supra* note 2, at 31.
[89] *See id.* at 170-171: 'the preventative sector targets criminogenic situations that can be altered in ways that make them less vulnerable to criminal events, less inviting to potential offenders. It analyses flows of people and the distribution of criminal events, identifying "hot spots", "hot products", and repeat victimization patterns and making them he focus for action. And while policing and penal solutions are part of its repertoire, the preferred remedy is to put in place situational controls and channel conduct away from temptation, rather than to bring prosecutions and punish offenders.' Cf also at 187: 'the most talked about developments of contemporary policing – the "broken windows" and the "zero-tolerance" approaches – imply a complete inversion of the old criminological assumptions. In today's criminology, minor offending matters, situational controls shape conduct, and deterrent penalties are a central resource for crime control.' Cf also the rationale for the UK RAE's Report on surveillance: 'We all also resent the emergence of the "surveillance society", yet demand that wrong-doers and terrorists are identified and apprehended *before* they can do mischief' (Royal Academy of Engineering, *supra* note 17, at 3, emphasis added).

3. Information-guided police care is capital intensive rather than labour intensive. Technological developments (miniaturization, wireless communication, capacity enlargement, broadband, merging systems and databases) have led to significant efficiency and improvements.

4. Information-guided police care is increasingly focussed on monitoring groups of potential suspects, for example, massive repeat offenders, organized criminals and terrorists, rather than individual suspects.

5. Information-guided police care is primarily focussed on crime prevention. Besides increasing fines and tickets (the enforcement efforts have greatly expanded) the police have applied a large number of innovative non-criminal enforcement strategies, varying from regular control actions (police control) of infrastructural junctions in big cities, specific controls of hotspots and target groups (nightlife) and, for example, signaling and advising the administration and other enforcement bodies on a more structural basis.

6. Information-guided police care creates relationships between information sources and decision-making processes that were previously separate.[90]

Along with a new focus on prevention and monitoring potential suspects rather than actual suspects, society's architecture is slowly being changed. This happens not only to prevent crime with real and metaphorical hinges and locks (a process that has been particularly visible, and effective, over the past 30 years or so) and 'a built environment designed to manage space and to separate people',[91] but also to better enable the detection of future crimes being planned or committed. This is a fundamental change. In the traditional paradigm, once a dead body was found, the police started looking for traces, witnesses, and other sources of evidence. Now, before a murder is committed, society is compelled to structure its systems in such a way that, should ever a murder be committed, evidence is more likely to be available. The major example of this re-structuring of society's architecture for crime-control purposes is data retention: in Europe, telecommunication providers have to store traffic data (who communicated when and where with whom, including which websites they visited) for a period of 6 to 24 months, so that the police is sure to detect criminal network structures and communication patterns in case a crime is committed at some point in the future.[92] Significantly enough, mandatory data retention has been enacted in the wave of post-9/11 antiterrorism measures only in Europe, but not in the United States, where the government is more restricted to impose serious administrative burdens on market parties.

Data retention is the first major instance of changing society's architecture purely for crime-control purposes. Although one should be careful with slippery slope theories, it is not unreasonable to see the precedential value of telecommunications data retention for other sectors in which important evidential data are processed, notably in the financial, traffic, private security (CCTV), and public-transport sectors.

Whether or not more data retention slips will be made down the slope, there is another, less visible but further-reaching, process in which the crime society's architecture is being changed. This is the treating of an emergent feature of a technology as mandatory in future architectures, ie the raising of a contingent side-effect of a technology to the level of an immanent characteristic. It has occurred most noticeably with, again, telecommunications. In its traditional form, the telephone happened to be easily interceptable, and this remained so until about the early 1990s. Then, due to increasing numbers of market parties and diversification of telecom technologies, the police suddenly started to have trouble in intercepting. Because a major investigation tool thus risked being lost, governments passed laws forcing telecommunication providers to build in interceptability.[93] Exemplary for this line of reasoning is a Dutch MP's statement: 'The traditional form of telephony can be intercepted. An alternative must be the same. We find that being interceptable is an *inseparable* part of

[90] Projectgroep Visie op de politiefunctie, *Politie in ontwikkeling. Visie op de politiefunctie* (Raad van Hoofdcommissarissen, NPI, 2005), http://www.politie.nl/Overige/Images/33_143611.pdf (last visited 19 February 2009), at 93-94.
[91] Garland, *supra* note 2, at 194.
[92] Directive 2006/24/EC, *Official Journal* L105/54, 13 April 2006.
[93] US: Communications Assistance for Law Enforcement Act, *see* http://www.askcalea.net (last visited 19 February 2009); Europe: Council Resolution of 17 January 1995 on the lawful interception of telecommunications (96/C329/01), *Official Journal* 4 November 1996, http://www.gliif.org/LI_legal/EU.htm (last visited 19 February 2009). For a comparison of the US and Dutch legislation, which again shows a more liberal approach to impositions on market parties in the US, *see* Koops and Bekkers, *Interceptability of telecommunications*, *supra* note 28 .

the phenomenon of telephony in our country.'[94] In a similar vein, when it turned out that cell telephones had the characteristic of 'knowing' their location, governments started to mandate in mobile phones the ability to make known their location in case an emergency number was called.[95] This has not occurred for crime-control but for safety reasons, but the result remains that locatability becomes an inherent feature of mobile phones and that as a consequence, generated location data will routinely become available for criminal investigation purposes. It is not hard to see that the same mechanism of 'essentialising' a contingent feature of technology in order to enhance control is at work here. This, equally effectively as mandatory data retention, shapes society's architecture in order to better monitor behaviour and therewith control crime.

5 The Crime Society: a Paradigm Shift in Criminal Law

The interrelated technological, socio-political, and legal trends I have outlined form the basis for what I propose to call the crime society. I use the term 'crime society' not in the sense of a society pervaded by crime in the sense of crime incidence, but a society that frames social interactions and structures – not only, but always also – in terms of crime and criminal law. The crime society is a society steeped in 'crime think' and 'crime control speak'. The expanding substantive and procedural criminal law and changes in society's architecture for crime-prevention purposes culminate in a surveillance society where criminal law is a primary, if not the foremost, form of social control. Its footprint is much larger than rising punishment and incarceration that are the result of increasing penal harshness: the shadow of criminal law, with its ubiquitous preventative surveillance and architectures, drops over all ordinary citizens in ordinary life.

This society is not different from the risk society or the surveillance society. It is just another way of looking at the current world. Beck, Lyon, and others have described recent developments and explained the world from certain perspectives, raising pertinent questions on what it means to live in today's world, and creating a solid basis for legal scholars to reflect on what regulation means in this world. The crucial role of criminal law in relation to the technological and socio-political developments has, however, not been articulated very prominently in current literature on risk and surveillance. I therefore think it is useful to complement the perspectives of the risk and surveillance societies with a cross-section of society from the perspective of criminal law. Conversely, the literature on the culture of control and penal harshness recognises the key role of criminal law, but tends to focus largely on incarceration and punishment. The increasing footprint of criminal law in the stages preceding trial and execution, not only with expanding investigation but also, crucially, in the preventative and architectural approaches of 'pre-investigation', is an aspect of the crime society that needs to be combined with the analyses of Garland, Lacey, and others.

Describing and explaining the 'crime society', which combines the risk, surveillance, and penal societies, enables us to ask pertinent questions on what it means to live in a 'crime think' world and what the implications are for governance of and through criminal law. This article provides no space for a comprehensive sketch of the crime society. I restrict myself here to noticing that the key trends (sketched above) have a major overall effect: a paradigm shift in criminal law. In the current – or perhaps already past – paradigm, criminal law as an instrument of social control is a last resort: to be handled with care and applied only when no other instruments avail. This paradigm is slowly being replaced by the crime society's new paradigm: criminal law is a first resort, to be handled whenever it is useful to control (perceived) social risks.[96] To be sure, the new paradigm has not (yet) fully replaced the old one. The constitutive elements of the criminal law paradigm – such as repression versus prevention, focus on individual suspects versus scanning large groups of unsuspected people – are located at a continuum, and neither the old nor the new paradigm are constituted by the exact extremes of the continuum. Yet a shift along the spectrum in all vital elements is unmistakable. Bearing in mind the developments sketched above, we can see the paradigm

[94] Parliamentary Proceedings Second Chamber [*Handelingen II*] 25 October 1995, 17-1123 (my translation, emphasis added).
[95] Phillips, *supra* note 9.
[96] Cf. Simon, *supra* note 2, at 14: 'often it is crime through which other problems are recognized, defined, and acted upon. (…) What is visibly different about the way we govern since the 1960s is the degree to which crime is a first response.'

shift under way in the move from the elements on the left to the elements on the right in Table 1:

In the old paradigm, criminal law:	*In the new paradigm, criminal law:*
is reactive	is preventative
focuses on harm	focuses on risk
focuses on moral wrongs	backs up regulatory interventions
investigates individual suspects	scans groups
collects concrete evidence for single cases	collects and shares raw data for profiling
relies on search and seizure	relies on statistics
centres on the criminal trial	centres on pre-trial (pre-)investigation
is enforced by the state	relies on public-private partnerships
aims at re-establishing order	aims at establishing order
follows society's architecture	shapes society's architecture
is a last resort	is a first resort

Table 1. The paradigm shift in criminal law

The table is a caricature of the paradigms, since both contain some elements of the other end of the spectrum, and not all opposites exclude each other. Criminal law is never purely reactive, nor can it ever be completely preventative. Few times and places exist where it was truly a last resort, and it can never be always a first resort for all social problems. The table indicates a spectrum along which criminal law can be situated. In legal doctrine, it was, until recently and often still today, situated largely in the left-hand column.[97] In practice, if not yet in theory, criminal law can be located at least in the middle and in several respects more towards the right-hand column of the spectrum. If current technological, social, and legal-political trends continue, sooner or later, criminal law will have altogether shifted from the left to the right, and a new paradigm will have emerged. Given the current situation and momentum, in countries like the US, UK, and the Netherlands it will be sooner rather than later. Actually, in Garland's analysis, the new paradigm is already there:

> the new crime control developments (…) play a role in *creating* that [late modern] world, helping to constitute the meaning of late modernity. Crime control today does more than simply manage problems of crime and insecurity. (…) In America and Britain today, "late modernity" is lived – not just by offenders but by all of us – in a mode that is more than ever defined by institutions of policing, penality, and prevention.[98]

The shift in criminal law from a last resort to a primary tool of social control has vast implications for regulation. The system of the law is based on the old paradigm, and instantiations of the new paradigm – often situated in the periphery of criminal law – do not easily fit the legal system. For example, mayors imposing area bans on loitering kids to prevent vandalism, public-private partnerships to block illegal content from the Internet, or using traffic controls with automatic number-plate recognition to make it unattractive for notorious recidivists to come to town – three illustrative examples of the new 'police care' – do not fit criminal law in the traditional sense: what crimes are solved here, what evidence is collected, who is being convicted? To accommodate the need for such new measures, a new legal basis and specific legal arrangements are created, on an ad-hoc basis, in a fuzzy combination of criminal, civil, and administrative measures with distinctly neo-criminal-law goals.[99] The classic system of criminal law moves, expands, and is patched up, to the extent that the old system can hardly be called a 'system' any longer.

[97] For example, Ashworth, *Principles* , *supra* note 45, at 54, argues that, '[i]n theory, the criminal law ought to be divided from civil sanctions and administrative regulation by reference to its censuring function, and by the principle – however uncertain in its application – that the ambit of the criminal law should be kept to a minimum.' *See* also, in terms of both content and structure, classic handbooks such as S.R. Cunningham, C.M.V. Clarkson and H. M. Keating, *Clarkson & Keating Criminal Law: Text and Materials*, 6th edition (London, Sweet & Maxwell, 2007); W.R. LaFave, *Criminal Law*, 4th edition (Thomson West, 2003); J. De Hullu, *Materieel strafrecht*, 3rd edition (Kluwer, 2006).

[98] Garland, *supra* note 2, at 194 (emphasis in original). For the Netherlands, R. Van Swaaningen, *Veiligheid in Nederland en Europa: een sociologische beschouwing aan de hand van David Garland*, 30 Justitiële verkenningen 9-23 (2004) also recognises many features of the new paradigm.

[99] *Cf.* Ashworth, *Principles* , *supra* note 45, at 55, arguing that ASBOs, being made in civil proceedings on application of local authorities or the police, are not a 'criminal charge', but can, when breached, be sanctioned as a criminal offence with up to five years' imprisonment – 'an ingenious scheme for imposing harsh punishments yet by-passing the appropriate protections at the crucial stage of the proceedings.'

Where policy and practice are thus effectively moving towards the new paradigm, theory and doctrine have to follow, by providing the new paradigm with a solid theoretical and systematic basis that it currently lacks. Of course, another strategy – the one most visible today in legal scholarship – is possible: to oppose the new paradigm where it undermines classical tenets of criminal law, and argue for limitations to the new 'police care' based on systematic legal arguments derived from the classical paradigm. This strategy, however, is not always effective and, I think, increasingly counter-productive, since it disregards the reality of the technological and socio-political trends that accompany the paradigm shift in criminal law. Law cannot change these trends, and it also cannot disregard them. This does not imply, however, that criminal law should it follow technological and socio-political trends without any resistance – constitutional law does set some limits to how criminal law can change. Technology and social and legal norms co-evolve. Rather than hang on to the old paradigm, legal doctrine and the legal system of criminal law should be revised and updated, after a critical reflection of the technological and social reality of the crime society. To illustrate the need for such reflection and revision, I will end this article by indicating some implications of the crime society for one of the basic elements of the legal system: legal protection.

6 Rethinking Legal Protection

6.1 The Traditional Focus of Legal Protection

In the traditional paradigm, legal protection has to perform the difficult balancing act of preventing innocents from being sent to jail while allowing those guilty of crimes to be convicted. The key tenet is that it is better to have ten guilty persons acquitted than one innocent person imprisoned. At least, that used to be the central tenet; these days, it sometimes appears rather the reverse.[100] Still, legal protection centres on the criminal trial, with investigation leading up to it and execution following it. In this paradigm, most attention is paid to the position of the suspect and defendant, and defence rights are the core of legal protection in the criminal law system. To be sure, with the rise of investigation powers the legal protection of unsuspected people in the pre-trial stage has also come to the fore, through requirements of probable cause and court orders before citizens' human rights, particularly privacy, can be infringed. In recent times, legal protection of victims has also emerged, even if victim rights are yet in their infancy compared to the body of defence rights. Altogether, criminal justice, in the old paradigm, is still very much a two-party process (prosecuting state versus citizen/suspect/defendant), with a well-developed system of legal checks and balances that allow the state to investigate, prosecute, and punish crimes while protecting citizens from overintrusive investigations and defendants from unjust convictions.

With the paradigm shift in criminal law, this system of legal protection shows increasing gaps. Of course, legal protection for defendants is still very relevant, but it is no longer adequate as the central focus of legal protection. In the crime society where all aspects of human behaviour are monitored and recorded on a routine and systematic basis, regardless of a concrete crime having been committed, legal protection should focus first and foremost on the citizen, not the suspect or defendant. Current protection mechanisms of citizens against intrusive government surveillance are ineffective, for a number of reasons:

- the on-going expansion of investigation powers in the politicised criminal law is rarely curbed by human-rights protection mechanisms; the European Court of Human Rights allows a large margin of appreciation for states to label measures as 'necessary in a democratic society', and the US Supreme Court is likewise reticent in setting considerable limits to new investigation methods;
- most investigation cases do not end up in court where they can be contested in the traditional way of enforcing legal protection rights;
- if they do reach the criminal trial, the exclusionary rule is applied in such a way that breaches of privacy do not imply a breach of the right to a fair trial if others' rights than the defendants' were at issue, such as privacy rights of citizens that happened to be infringed along the way;[101]

[100] *Cf.* Garland, *supra* note 2, at 192: 'The prevailing attitude is that it is better to keep a known criminal locked up for ever than to risk the life or property of another innocent victim.'

[101] ECtHR 12 May 2000, *Khan* v *United Kingdom*, No 35394/97. In the US, the exclusionary rule 'has lots and lots of exceptions', and in *Hudson* v *Michigan*, 547 U.S. 586, 126 S.Ct. 2159 (2006), the Supreme Court suggests that changed circumstances have rendered the rule obsolete, *see* D.A. Sklansky, *Is the Exclusionary*

- citizens' legal protection is linked to criminal prosecution and focuses on whether or not privacy-infringing actions can be taken for evidence gathering; this is not tailored to pre-investigation practices of collecting, storing, and mining data for profiling purposes, nor does this system aim at protecting citizens from injustices *outside* the criminal investigation process, for example, when data collected and stored for criminal risk governance may be used for decisions regarding employment, insurance, housing, banking, or setting up a business;
- the potential harm for citizens is no longer restricted to concrete physical or emotional damage to home, body, or close relationships, but also includes vague, invisible, and long-term forms of harm resulting from 'data shadows' lingering in public and private data bases; perhaps the core vulnerability is no longer sending an innocent person to jail, but labeling the digital persona of an innocent citizen with a stamp that significantly lowers the quality of her future social life;[102]
- in the current theory of legal protection, the citizen is a rational and accountable subject whom the government, in principle, trusts to behave lawfully, but in the practice of criminal risk governance, the citizen is becoming an object of control untrusted by its government;[103] this requires a fundamentally different type of protection mechanisms.

6.2 Contours of New Forms of Legal Protection

When updating legal protection to meet the new reality of the crime society, we should of course not throw away the baby along with the bathwater. Defence rights to protect defendants from unjust conviction, and privacy rights of citizens against overintrusive criminal investigation remain very important. However, these should be supplemented with new forms of legal protection that fill in the emerging gap in protection of citizens against the ever-expanding footprint of criminal law in the risk and surveillance societies. A systematic rethinking of legal protection in the crime society requires substantial reflection, research, and debate. As input for this rethinking, I will sketch some contours that I think should show up, without pretending to paint a comprehensive picture.

A key feature of the new paradigm is the switch from repression in individual cases to risk control in general. This should be mirrored in the protection paradigm with a similar switch: from preventing government abuse in individual cases to generically controlling the criminal justice process. This runs as a red thread through the new forms of legal protection.

For example, the primary stress in current debates on privacy and data protection, highlighting data minimisation and purpose specification as crucial elements in preventing government abuse, distracts attention from what is happening in real life. Minimising collection and processing of data simply does not fit the new paradigm of the multi-purpose monitoring of information junctions. To quixotically hold on to Article 8 of the European Convention of Human Rights, the US 4th Amendment, and data-protection or fair information principles as the key instruments to check the power of law enforcement may be noble but it is largely ineffective. Privacy and data protection should be complemented by an invigorated attention to non-discrimination, fair treatment, and correcting abuse of power. In the crime society, information more than ever wants to be free: data *will* be collected and processed, whether or not in compliance with data-protection principles. In such a world, it is no longer feasible to *prevent* data processing, but it becomes crucial to *control* data processing. Protection mechanisms known from the anti-discrimination field – reporting and complaint mechanisms, internal auditing, ombudswomen, focusing on decisions that affect people's lives – should be incorporated into the daily practice of criminal risk governance. To be sure, such mechanisms already exist to some extent, but in their current forms, they are peripheral rather than core procedures, and they need substantial increase in powers and resources to become really effective in the new paradigm.

Rule Obsolete?, 5 Ohio State Journal of Criminal Law 567-84 (2008) . Sklansky, at 582, notes that the exclusionary rule needs to be supplemented by other forms of legal protection, 'particularly for that vast category of police conduct that is not aimed at obtaining evidence for use in court.'

[102] It is this aspect that Solove stresses in suggesting to replace the trite metaphor of Orwell's *1984* by Kafka's *The Trial* as the relevant nightmare scenario for 'the digital person'; *see* Solove, *supra* note 81, Ch. 3.

[103] 'Privacy plays an important role in the social contract between citizen and state: to enjoy a private life is to act on the assumption that the state trusts the citizen to behave in a law-abiding and responsible way. Engaging in more surveillance undermines this assumption and erodes trust between citizen and state (…) with the citizen living under the assumption that he or she is not trusted by the state to behave within the law', House of Commons Home Affairs Committee, *supra* note 41, at §9; *see* also Van den Heuvel, *supra* note 39, at 89.

This does not imply that data minimisation and purpose specification should be discarded outright. Basic limits determining who may process what data will still need to be set, for example, to prevent data obtained with police automated number-plate recognition systems for monitoring who enters and exits a city from being passed on to employers who might be interested in the whereabouts of their employees (or their cars). Since it is difficult indeed to enforce the purpose-specification principle in practice and to prevent function creep, we should no longer rely only on law in the books but also on law in the technology, that is, to build-in in technology those legal limits that we find crucial to uphold.[104] Rather than aim for *overall* data minimisation and purpose specification that only work in theory but not in practice, setting *some* limits to data processing that will be enforced in practice because they are embedded in the data-processing systems and procedures themselves may be a way to find a new balance in the citizen-law-enforcement relationship.

In a similar vein, the shift from treating citizens as a priori trustworthy subjects to treating them as a priori untrustworthy objects should be accompanied by a shift to organised distrust throughout the criminal justice system. That is, rather than rely on legal protection to curb excesses of government intrusion in exceptional, individual cases, legal protection should ensure permanent and ubiquitous control of criminal law enforcement. When crime control shifts from criminal investigation of committed crimes to criminal risk governance,[105] the cornerstone of legal protection is no longer the judge who checks power abuse in court or during criminal investigation, but the accountant who audits the correct, fair, and transparent functioning of the law-enforcement system at large. Where in the new paradigm, criminal law in the traditional sense makes room for administrative law, both substantively and procedurally, legal protection should take the form of administrative checks and balances. Supervisory bodies, administrative courts, and ombudswomen are better suited than the criminal court to check the power imbalance inherent to the new 'police care'. This also allows for more flexibility in calling 'criminal risk managers' to order, since these may be bureaucrats of public-private partnerships as soon as traditional police officers.

To conclude, in a new system of legal protection that is devised to meet the emergence of the crime society, legal doctrine has to search for a new central adage. 'It is better to have ten guilty persons acquitted than one innocent person imprisoned' (or vice versa, depending on the political climate) no longer exemplifies the crucial trade-off of criminal justice. A revealing thought exercise is to devise a better-suited adage in the age of the crime society. Perhaps something like: "It is better to not prevent one crime from being committed than to cause the loss of ten QUALYs to innocent citizens"?[106]

7 Conclusion

In this article, I have sketched the contours of the emerging crime society, as an important but relatively underrated perspective to look at late modern society, to complement the well-known perspectives of the risk society and the surveillance society. It also ties in with Garland's 'culture of control', but it looks at this culture from a somewhat different angle: the increasing footprint of criminal law is not only much broader than increasing penal harshness, and not only disproportionately burdensome to the poor and to minorities (Garland's main concern), but it also affects ordinary citizens in daily life in their relationship with the government. It is the combination of the risk and surveillance societies, with their preventative and architectural approaches to criminal (pre-)investigation, with the criminal-law-pervaded

[104] On the opportunities and threats of using technology as a regulatory tool, *see* E.J. Dommering and L. Asscher (eds), *Coding Regulation. Essays on the Normative Role of Information Technology* (The Hague: T.M.C. Asser Press 2006) and R. Brownsword and K. Yeung (eds), *Regulating Technologies* (Oxford: Hart Publishing 2008). For an argument why law in the books needs to be complemented by law in the technology, *see* M. Hildebrandt and B.-J. Koops (eds), *D7.9: A Vision of Ambient Law* FIDIS 2007).

[105] *Cf.* Van Swaaningen, *supra* note 98, at 20: 'The police will develop more and more into a risk manager and information broker' (my translation).

[106] A QUALY is a Quality-Adjusted Life Year, a measure used in health policy for cost-benefit analysis of medical interventions. It measures the increase in number of years lived, adjusted for the (health) quality of these years, and offsets this against the cost of the treatment. Such a type of measure might be useful in criminal risk governance to make transparent the number of years a citizen is affected by a crime-control intervention, adjusted for the loss of quality in her life, for example, when she is forced to move and look for a new job because her neighbourhood makes life impossible after the policy asked around rather conspicuously whether people knew things that might confirm her fitting the profile of a terrorist that the data mining computer came up with. Perhaps superfluously, I mention this not as a proposal for criminal risk calculus, but as a metaphor to indicate the need for a new way of thinking about vulnerabilities of citizens in the crime society.

development of penal harshness, that constitute the 'crime society'. This perspective is perhaps most closely related to Jonathan Simon's notion of 'governing through crime'.[107]

I have also articulated the pivotal role of technology in this process. The same technologies that characterise and form late modern society as complex, mobile, diversifying, metropolitan-anonymous, and globalising, also facilitate, to a quickly increasing extent, the monitoring of all social processes. Technologies for streamlining data flows, including merging databases, together with risk control processes as evidenced in the new paradigm of intelligence-led 'police care', imply that criminal investigation authorities, in principle, stand at the junction of all sectoral surveillance societies and have the power, if not yet the practice, to access all imaginable data that are stored in today's myriad monitoring processes.

Thus, technology is a natural ally of the crime society, through the combined effects of criminalisation, expanding policing, preventative and architectural approaches, and the surveillance society that technology all facilitates. We are moving ever nearer to a crime society in which each and every form of human behaviour is perceived in terms of potential criminal risk and controlled by means of criminal law.

The role of technology in this process is often facilitating, but also in developments where it is not a partial causative factor, technology plays an important role: its relentless storage and memory capacities make a quantitative and qualitative difference as compared to traditional policing by people. The pivotal role of technology is therefore important to add to the analysis of 'governing through crime', which so far tends to build on legal and socio-political rather than technological developments.[108] These legal, socio-political, and economic developments, although we should not underestimate their institutional path-dependence, do not necessarily lead to an ever-increasing criminalisation of society.[109] Technology, however, might provide a compelling turn of the screw. Often, technological processes are irreversible: once an infrastructure is built for monitoring a certain process, it is very hard to dismantle it and to revert to older types of control. CCTV, national identity numbers and cards, biometric passports, DNA data bases, interceptable telecommunications, and many more infrastructures soon become institutionalised and ingrained in society, to the point where it becomes pointless to ask whether we can do without them. They are only replaced by new infrastructures if these provide an equal or even better functionality. This has serious implications for the way we deal with these developments. The potential negative consequences of the technology-pervaded crime society have to be addressed by organising new countervailing powers and new checks and balances, rather than trying to put genies back in bottles.[110]

The paradigm shift in criminal law – from a last resort to a primary tool of social control – goes hand in hand with a shift in the power balance between government and citizens. Traditional boundaries – both spatio-temporal (walls and clothes, human effort to search and seize) and legal-systematic (evidence of a crime, probable cause against individual suspects) – make way for new, more vague and fluid boundaries, allowing the government – and increasingly private parties – to penetrate deeply into the private sphere of citizens who have not done anything wrong (yet). Trust cedes to distrust as default in citizen-government relationships. Criminal risk control focuses on multifarious other means of control apart from trial and imprisonment. All this implies that citizens are becoming more and more transparent to the government, and that they can suffer in more ways than damage to property or loss of personal freedom through incarceration. The digital personas that accompany and mirror citizens in the information society are vulnerable in the new forms of 'intelligence-led police care' to error and misinterpretation, not only by law-enforcement agencies but also by other public and semi-public institutions that rely on data bases. As a result, the citizens of the crime society can no longer merely rely on the traditional legal protection that is embedded in the old paradigm of criminal law to protect them from overintrusive government scrutiny or abuse of power.

These insights enable us to answer the question that I posed at the beginning: what are the implications of the technology-facilitated criminalisation of society for the legal protection of citizens? The legal protection embedded in the system of criminal law has to be rethought and revised, now that the paradigm of criminal law itself is shifting. I have indicated some

[107] Simon, *supra* note 2.
[108] *Id.*
[109] Lacey, *supra* note 45.
[110] *Cf.* D. Brin, *The transparent society: will technology force us to choose between privacy and freedom?* (Reading, Mass.: Perseus Books 1998).

outlines of possible new checks and balances, which centre on a shift from preventing government abuse in individual cases to generically controlling criminal justice. Apart from continuing to ensure a balanced investigation of concrete crime cases and a fair trial, the advent of the crime society also calls for a permanent and ubiquitous control of criminal risk governance, by embedding organised distrust throughout the criminal justice system. Additional administrative and accountancy-type checks and balances, with adequate funds and powers, have to be installed to audit correct, fair, and transparent functioning of the law-enforcement system in the age of the crime society.