Reference to this paper in APA (6th):
Dahl, J. Y. & Sætnan, A. R. (2009). "It all happened so slowly": On controlling function creep in forensic DNA databases. *International Journal of Law, Crime and Justice, 37*(3), 83-103.

“It all happened so slowly” – On controlling function creep in forensic DNA databases.

Johanne Yttri Dahl
Research fellow
Department of Sociology and Political Science
Norwegian University of Science and Technology
7491 Trondheim, NORWAY
Tel. +47 91 73 49 64
Fax. +47 – 73 59 15 64
Email: johanney@svt.ntnu.no

and

Ann Rudinow Sætnan
Professor
Department of Sociology and Political Science
Norwegian University of Science and Technology
7491 Trondheim, NORWAY
Tel. +47 – 73 59 17 86
Fax. +47 – 73 59 15 64
Email: annrs@svt.ntnu.no

Johanne Yttri Dahl will be handling all correspondence.

“It all happened so slowly” – on controlling function creep in forensic DNA databases.

Forensic DNA databases are implemented worldwide and used increasingly. Part of this increasing usage is arguably a matter of function creep. Function creep refers to changes in, and especially additions to, the use of a technology. In this article we explore the notion of function creep as we discuss why and how it has taken place on forensic DNA databases. We also consider what future function creep it is possible to envisage. As even security enhancing technologies may contribute to insecurities, what safeguards should be in place to render function creep governable? We use the Norwegian DNA database, expanded considerably as recently as September 2008, as our primary case for discussion. Additionally we use examples from the English and Welsh DNA database which, considered world leading, may be an indication of where other DNA databases are heading. The article isn’t data-driven but draws on a wide spectrum of data: governmental documents, public and Parliamentary debates, and interviews.

“It all happened so slowly” – On controlling function creep in forensic DNA databases.

”Asking questions about the process of surveillance creep and possible latent goals should be a central part of any public policy discussion of surveillance before it is introduced. Beyond determining if a proposed tactic is morally and legally acceptable, works relative to alternatives and can be competently applied, it is appropriate to ask, once the foot is in the door, where might it lead?” (Marx 1988: 387)

This is an article about function creep in the use of forensic DNA-databases. Function creep refers to changes in, and especially additions to, the use of a technology. When personal data, collected and used for one purpose and to fulfill one function have migrated to others that extend and intensify surveillance and invasion of privacy beyond what was originally understood and considered socially, ethically and legally acceptable[1] it is known as function creep. The term is frequently used when discussing surveillance technologies or surveillance uses of technologies with other purported primary goals. One of many surveillance technologies that has been subjected to function creep is forensic DNA databases. Since DNA was first used in forensics during the mid 80s, it has been used increasingly, and forensic DNA databases have been and are still being established and developed all over the world. Not only that, but: “No country has yet ever reduced its established forensic DNA collection or sought to curtail its uses once it has been embedded successfully into its criminal justice system” (Williams and Johnson 2005: 16). While the use of DNA in forensics in the

[1] http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf (last accessed 16.10.08) p 9

beginning was considered quite controversial, there has been a trend that legal restrictions regarding forensic DNA databases have been loosened – function creep has taken place.

One of the main reasons for this function creep is that forensic DNA technology is considered an efficient tool in criminal justice matters, one that contributes to increased security. In this article we will look at: Why and how does function creep occur? Why, when and how might we wish to prevent or stall it? What function creep has taken place on (the Norwegian) forensic DNA database, and through what processes? What future function creep is it possible to envisage? And, as even technologies implemented to increase security may contribute to insecurity (Aas et al. 2008); what safeguards should be in place to render function creep governable? First we will dig deeper into the concept of function creep, then we move on to present the data that the article is drawing from and some methodological reflections, before we present some of the function creep that has taken place in relation to forensic DNA databases and what safeguards we consider beneficial to enable a fairly governed DNA database. The use of the Norwegian forensic DNA database was recently expanded considerably; therefore it will be used as a case for our discussion. However, as Williams and Johnson (2004a: 9) write, the history of the UK National DNA Database (the NDNAD) is a history of continuous expansion. The NDNAD is considered one of the leading, if not *the* leading, forensic DNA database in the world. Norwegian authorities have pointed to the UK and sought to follow in the UK's footsteps. Thus, even from a Norwegian perspective, we consider it helpful to use examples from the NDNAD in our discussion, not least as an indication of where the Norwegian forensic DNA database might be heading.

1. Function creep: What is the concept?

Fox (2001: 261) defines *function creep as* "previously authorised arrangements … now being applied to purposes and targets beyond those envisaged at the time of installation". While function creep may be the most common term, several others are used to describe the same, or nearly the same phenomenon. *Surveillance creep* is one such. Marx (1988) writes:

> *"As powerful new surveillance tactics are developed, the range of their legitimate and illegitimate use is likely to spread. Where there is a way, there is often a will. There is the danger of an almost imperceptible surveillance creep"* (Marx 1988:2).

Seventeen years later, in 2005, the term is as relevant as ever and Marx writes:

> *"A fascinating aspect of surveillance technologies as hegemonic control involves their tendency to expand to new goals, agents, subjects and forms. The surveillance appetite once aroused can be insatiable. A social process of surveillance creep (and sometimes gallop) can often be seen. Here a tool introduced for a specific purpose comes to be used for other purposes, as those with the technology realize its potential and ask, 'Why not?'"*(Marx 2005: 386).

Innes uses the term *control creep* and defines it as follows:

> *"Control creep captures the sense in which the apparatus of social control, that is the combination of technologies and instruments designed to respond and to regulate*

deviant behavior, are becoming increasingly dispersed and interspersed throughout many different arenas of late-modern social life" (Innes 2001: 2).

With this Innes (2001: 2) intends to *"Capture something more profound, than just an expansion in the monitoring of social life"* as covered by Marx' (1988) term *surveillance creep*.

Williams and Johnson (2008: 82) uses both function creep and control creep and writes as follows: *"... describes how a government's programme of technological intervention into social life is gradually, incrementally, but deliberately, increased over time*".

All the terms refer to function change, especially expansion, and especially expansion of surveillance and control functions. All include the word "creep". While not all function expansions are "creepy"[2], we do have these terms for function expansion that are negatively loaded, carrying a hint of "sneakiness". We see this as in part referring to the social effects of certain functions, in part to the process through which they were implemented, and in part to interactions between effects and implementation process.

The declared function of these technologies – surveillance – can sometimes be regarded as "creepy" in itself, a sneaky peering into others' lives the better to control them. But surveillance and social control are also necessary, often positive, aspects of society. The challenge, then, is to define and maintain acceptable forms and levels of surveillance and social control. Sometimes the addition of a new function to a technology is, all things

[2] Webster's Encyclopaedic Unabridged Dictionary of the English Language (1994: 342) "1. that creeps, as an insect. 2. having or causing a creeping sensation of the skin, as from horror or fear."

considered, a good thing. How we categorize a function expansion is a value judgment. The next question, then, is how we go about making such judgments.

"Creep" can refer to a secretive, sneaky process of change. How democratic or undemocratic the function implementation process has been may also be linked to the outcomes -- how we see a given function as affecting distributions of power, autonomy, knowledge, access to resources. But the term may also simply refer to slow, crawl-paced change, which may be a good thing as it allows time for reflection, debate, and democratic process. So not all function expansion warrants a derogatory term, but "creep" need not always be derogatory. The term *function creep* may in a given case refer to the skin-crawling, chilling nature of the latest added function and/or the sneakiness of an undemocratic, secretive process of socio-technical change … but it may also simply refer to slow, considered, and accepted change. In this article we will focus primarily on process and the consequences of process for outcomes. We have chosen to use the term "function creep" with its ambivalent implications – potentially both positive and negative – rather than "surveillance creep" or "control creep" where the power aspects of "surveillance" and "control" highlight the negative implications of "creep".

Function change and expansion occur because they can. They occur because technologies are interpretatively flexible (Bijker 1995) and their users imaginative and creative (Oudshoorn and Pinch 2003). Surveillance technologies are socio-technical systems for gathering, storing, accessing and analyzing information (so: information systems) about the appearances, communications and actions of human subjects. Information systems are considered to be among the most interpretatively flexible (Bijker 1996). Information systems are highly flexible because not only can their material tools (computers, routers, servers, screens) be used in multiple ways, but so too can their information content. Regarding DNA, genetic

information is already used for medical diagnostics and research, paternity testing, forensic identification, inferring prehistoric migration routes … and further future uses have been predicted. The material structures of the databases can serve to safeguard DNA information or to share it, to aggregate it or to search out individual cases, and so on.

1.1 OK, functions creep. What are "functions"?

The term *function* is used in many contexts with slightly different implications. One context relevant here is information technology (IT) engineering. For IT engineers, defining the functional parameters of a proposed IT system is a routine task. In this context we meet a fairly simple, almost mechanical definition of *function*: a segment of program that carries out a particular movement of data – register, code, store, search, collate, print -- as represented in the iconography of task and/or information flow charts (see e.g. Bræk et al. 1982). This definition says little or nothing about what the data are used for or to what social effects.

When the data registered are personal data, data protection laws come into play. Here we meet a second meaning of *function* in the form of a synonym: purpose. One of the basic tenets of data protection laws is that data collected for one purpose may not be used for any other purpose without seeking new consent and/or concessions/permits (see Norway's Personal Data Act, Ch. II, section 11, §§b and c[3]). This too is a rather formalistic, almost mechanical definition, and one that is critiqued from two sides. In the case of medical research those who gather and use personal data are often frustrated by the rigidity of this rule, claiming that potentially valuable data analyses and reports are hampered by it (Hofmann 2005). At the same time, privacy advocates find the rule inadequate, since many data usages they perceive as qualitatively new and different, can nevertheless be characterized as serving an already

[3] http://www.datatilsynet.no/upload/Dokumenter/regelverk/lov_forskrift/lov-20000414-031-eng.pdf

established purpose. When a DNA-database initially presented as a tool for solving serious crimes is expanded to cover volume crimes, is that a new purpose or still the same one: Catch as many criminals as possible?

Taking privacy advocates' point into consideration, we might want to move our definition towards a sociological understanding of *function*. Without committing ourselves to a Structural-Functionalist standpoint, we can say that in Sociology more broadly the function(s) of a social phenomenon (an artifact, a practice, an institution, etc.) is/are the social effect(s) of that phenomenon Within Structural-Functionalism, function (as opposed to dysfunction) refers more specifically to effects that contribute to the continuity and cohesion of society, which in turn is presumed to be a desirable outcome (Mathiesen 2001: 277). But the concept is also used more broadly, including in more conflictual views of society (Mathiesen 2001: 277), to be any effects on the social fabric. Incorporating this view into the two above, we can say that each function of an information system, such as a DNA database, is a data processing routine with some social effect(s). These effects may be positive or negative or mixed, negligible or dramatic, and there may be no consensus as to which.

That brings us to one last point: When is a function new? Given the definition we have chosen, we could say that a function is new when its social effects are new, but that does not entirely solve the problem. After all, there may not be consensus on that issue. But perhaps that is an adequate definition nonetheless. It leaves the matter in the arena of political discourse, which may be precisely where it belongs. A function is new when a data-processing routine or goal is added, subtracted, or changed to a degree that arguably has new social effects. Those who perceive a function as changed, are then left the task of arguing that point. There are, however, some signposts that might signal a functional change, such as when

a given data-processing routine requires dispensation from current regulations, or breaks with a promise used to gain acceptance for the database in the first place.

1.2 Technology is neither good nor bad … nor is it neutral [4]

It can be taken as given that no technology is ever perfectly good or perfectly evil (Collins and Pinch 1994:150). "Although there is no doubt that the benefits of technological progress have vastly improved human conditions in many ways, technology also carries risks" (Yuthas and Dillard 199: 48). Even technologies implemented for security-enhancement may contribute to not only security, but insecurities as well (Aas et al. 2009). Zedner (2009: 263) makes this point using the example of "The Sorcerer's Apprentice"[5]:

> *"Policy makers may act as modern-day wizards conjuring new technological alchemy as the magical charms with which to cure the ills of the contemporary world. But as the Sorcerer's Apprentice learned the hard way, these spells may prove more powerful and less controllable than their makers anticipate – less charm one might say than hex. The temptation to seek technological solutions is rarely accompanied by sufficient anticipation of the fact that technologies may develop unpredictably or be subverted in ways that render them greater sources of insecurity than security."*

This capacity for good and/or evil does not reside in the technologies alone. Technologies do not determine their own fates. Technologies are only used when they are perceived (at least

[4] Kranzberg's first law of technology (Kranzberg 1986).
[5] Most readers will be familiar with the Disney version of this tale, in which Mickey Mouse casts a spell so that the broom will do his sweeping chores for him, but then loses control.

by some) as producing desirable results. But this need not imply that technology implementation and outcomes are results of some sort of conspiracy. While human choices are certainly consequential, technologies have material properties that are amenable to certain uses and resistant to others, including some that may come as surprises to us all. "Unanticipated uses and side effects of innovations can never be fully foreseen or controlled, and technologies we use today can have serious consequences for individuals separated from us by great expanses of time and space. Although the risks can never be eliminated, we must own up to their possibility and make serious attempts to anticipate and control them" (Yuthas and Dillard 1999:48).

Garland (1995) argues that surveillance technologies are essential and inevitable in complex societies. In his view, they are not themselves the problem; rather, the issue is how they can be regulated to avoid abuse. While it is almost certainly impossible to foresee, let alone prevent, all future applications of a given new technology, we consider it worthwhile to discuss how such expansion might be governed. The main goal of the article is to discuss: *What safeguards need to be in place to govern forensic DNA databases?*

2. Methods

Function creep evolves over time. Therefore the past, the present and the future are all relevant for discussing it. Looking from the past to the present enables us to see what kind of changes have taken place in the usage of forensic DNA databases. However, wanting to debate how to govern function creep not only at the moment, but also with an eye to the consequences of our decisions, we need to try to raise our gaze from the present to the future. We agree with Haggerty (2009) that interests in surveillance have solidified a belief that we must seriously consider what lies ahead if we are to advance towards collective goals, or

recognize looming disasters. Our article is not an exercise in prediction, but a reflection on possible alternative futures.

As the past, present and future are all relevant for this article we see the need to draw on a large spectrum of data, all various forms of texts arts. The data include governmental documents (White Papers from Norway and reports from the British Home Office), public and Parliamentary debates, and interviews with Norwegian and British stakeholders in the DNA debate; lawyers, police, politicians, privacy interests, expert witnesses and DNA-laboratory workers. A total of 30 informants were interviewed. The use of governmental documents as data enables us to view aspects of the debate (or lack of it) regarding DNA-databasing and expansions of it. The informants for the interviews are a strategic sample, chosen on the basis that they were knowledgeable on the subject and represented a variety of perspectives on the use of DNA-databasing. The interviews were semi-structured. This provided the opportunity that both the informant and the interviewer could influence the direction of the interview. This is particularly important when talking about possible future events because what one thinks will happen in the future is very individual.

In spite of drawing on a wide spectrum of data, this is not a data-driven article. Rather it is driven by our understanding of function creep – why it occurs and how it might be controlled. We are using our data not to test hypotheses or claims, nor to establish predictive rules, nor to measure the relative strengths of various function creep drivers and controlling instruments. Rather, we use the data eclectically to illustrate what we think are clear instances and circumstances of function creep and thereby to propose potential means of governing it. More stringent tests of our proposals may be appropriate in future research.

While the Norwegian DNA database is the main case of the article, we use data about the UK NDNAD as a comparison case, since it is used as a reference point – be it as inspiration or object of criticism – not only in Norway but also by stakeholders in many other countries (Williams and Johnson 2008).

3. Why function creep takes place and some of the safeguards we need to govern it

Function creep occurs through a number of mechanisms. For instance, we often see technologies introduced when conditions are taken to indicate a dire need, then gradually expanded into less urgent usages. This need not come about conspiratorially. It may also come about in spite of everyone's best intentions, for instance through uncritical optimism and because the moral terrain shifts as soon as the initial investment is made. Once a technology is in place, it becomes wasteful not to use it to the fullest acceptable limit. Usages that might not have been sufficiently legitimate for initial implementation do have sufficient legitimacy to be tacked on later. In other words, there is no need to shout "Wolf! Wolf!" We do not need to assume a conspiracy. The best of intentions may lead us in directions and distances we, in retrospect, did not wish to go.

So let us assume good intentions. Obviously, good intentions are insufficient as a means of controlling the spread and direction of function expansion. So what measures can we take to support our good intentions? In the following we will discuss what safeguards – or measures – that might be helpful to govern forensic DNA databases. For each measure we will also discuss examples showing how, why, when these have been used or might advantageously have been used. None of these measures would of themselves guarantee a "good" outcome.

Not only do we need to combine measures because each has its own innate weaknesses, but we also need to accept that in the final analysis we may not all agree on what outcomes are "good". While we are aware that no degree of democracy can insure a perfect society, we aspire to look for ways to make the process of technology development, including function expansion, more democratic and less "creepy".

3.1 Assess necessity and effectiveness

In Norway all work preparatory to official reforms and changes in laws or regulations has to follow specific instructions. The instructions are intended to ensure that financial, administrative and other significant consequences of reforms and measures are clarified. The instructions are also meant to ensure that institutions responsible for the matter assess all relevant and significant consequences, and that stakeholders and the general public are included in the decision-making process before a decision is made (Instructions for Official Studies and Reports 2005). These instructions have been followed in the process of expanding the Norwegian DNA database. But while this is a comfortingly democratic process, it may nevertheless be a flawed one. Democracy needs to be used actively lest complacency allow decisions to pass that we would not have accepted had we thought them through.

One of the main arguments made by Norwegian politicians in promoting expansion of the Norwegian forensic DNA database has been its purported efficiency in solving crimes. In a press release, the Ministry of Justice (2007) stated that no method can outperform DNA, neither when it comes to efficiency nor credibility and that it is necessary for the Norwegian police to have efficient tools like police elsewhere. Repeatedly, DNA advocates predict that DNA will contribute to increased detection of a variety of crimes from volume crime, serious crime, organized crime, national as well as international crime. Consequently, increased use

of DNA will free up police resources. Moreover, the ability to detect more crime will contribute to increased levels of security (Storberget 2007).

We don't doubt that the use of forensic DNA databases may be useful and effective, but it may not be as efficient as claimed. It has been claimed in official documents[6] and debates in the Odelsting[7] that detection rates on volume property crime in the UK increased from 14 to 45 percent where the DNA database could be used. Through this and similar arguments using statistics it becomes evident that Norwegian politicians have read reports from the British Home Office such as the "DNA Expansion Programme 2000-2005: Reporting achievement" and been seduced by the apparently impressive statistics. Where Norwegian politicians have erred, however, is in comparing the general detection rate to the detection rate where the NDNAD was used (Dahl and Lomell forthcoming). Equating the two gives a deceptive impression that the general detection rate will increase dramatically by expanding the DNA database. What the numbers actually show is that in 2004/05 there were 5,6 million recorded crimes in UK. Of these, 913 717 were subject to crime scene detection, which resulted in 49 723 crime scene DNA profiles being added to the NDNAD. Even assuming one profile per crime scene, DNA was only loaded from 0,88% of crime scenes. It is in this 0.88%, that a 40% detection rate was reported. I.e. only 0,35% of crimes were detected using DNA (GeneWatch 2006a: 8). In the Norwegian debate there appears to be a lack of mathematical competence, perhaps exacerbated by technology optimism and a lack of skepticism, a lack of critical reflection regarding who are the providers of these numbers and what their objectives may be.

[6] http://www.regjeringen.no/nb/dep/jd/pressesenter/pressemeldinger/2007/auka-bruk-av-dna-for-a-oppklare-meir.html?id=482547

[7] The chamber of the Parliament that proposes new laws.

This example illustrates how the forensic DNA database is subjected to an expansion and function creep as a result of a political investment, and how one of the most often used forms of arguments, statistics, is flawed (Dahl and Lomell forthcoming). This shows how important it is that necessity and effectiveness are evaluated before, but also during the use of forensic DNA databases. It also shows how important it is that such evaluations are done by organizations without self interest in the results. When implementing any technology, forensic DNA databases included, it is important to have procedures for function evaluation – pre- and post-implementation.

Furthermore, not only initial implementations should be thoroughly evaluated. If we wish to govern function creep, each additional function should be discussed, not only regarding necessity and effectiveness, but also according to ethical questions. It is important that new functions are evaluated and discussed publicly. Merton (1942) points out how "organized skepticism" is a key element in the practice of science, helping science to avoid, catch, and correct its humanly inevitable errors. We might say the same of democratic society as a whole.

3.2 Laws and regulations

Democracies are based not only in debate, but also in law. Norway's oldest codified laws – the 13th century *Frostatingsloven* – include the sentence, a familiar motto to this day: "Med lov skal landet byggjast, og ikkje med ulov oydast" [Through law shall the nation be built, and not by unlawfulness destroyed.]. This faith in the law as a guarantor of justice, fairness, and social stability is characteristic of democratic societies in general, not only of Norway.

We have already seen above that the law requires some degree of reflection and some balance between conflicting interests before taking the first step towards implementing a new

technology of such proportions as a national forensic DNA database. That process of consideration may point out some number of concerns and misgivings about the new technology. Frequently we see that such concerns are "met" by proposing that implementation of the new technology be contingent on certain legal restraints. Yes, we will have a national DNA database, but the law will limit who will be registered, who will have access to the database, what purposes the database will serve, and so on.

In Norway, as in most other countries, a number of laws and regulations govern the forensic DNA database, for example when it may be used and who may be registered. When the database was first established in 1999 the law only allowed registration of people convicted of severe crimes, such as murder, sexual offences, robbery and grievous bodily harm. A White Paper (NOU 1993:31) concluded that including people convicted of these crimes would be appropriate and sufficient and that the main goal was "that the detection rate will become as high as possible when it comes to punishable actions, and naturally especially when it comes to severe crimes that threaten other peoples' life and health" (NOU 1993:31 p 7, our translation). In 2005, 12 years later, a new White Paper concludes that there is a need to expand the Norwegian DNA database (NOU 2005:19). This expansion is also linked to an expansion of its goal. Now it is to be used also in the fight against "volume crime"[8]. As of September 2008 it is no longer only people convicted of serious crimes who may be registered, but anyone convicted of a crime that may lead to imprisonment[9]. This could include people convicted of speeding, white-collar crime, and draft-dodging. People suspected of crimes, but not convicted, are to be registered on an investigation database that may be searched against the evidence database.

[8] http://www.regjeringen.no/upload/JD/Vedlegg/Faktaark/DNA_reform_web.pdf
[9] However, fear of having an explosion of cases to deal with has lead to regulations that only people convicted to imprisonment for over 60 days will be registered for the time being (Riksadvokaten 2008).

What are the social effects of such a change? “DNA profiling and DNA banking enable the construction of ‘closed circuit’ of surveillance of a defined population” (Williams and Jonson 2004a: 1). Once inside the database, you are constantly on a “virtual line-up” of potential suspects. The larger the database, the larger the portion of the population subjected to this more or less constant surveillance. The larger the scope of crimes that lead to searches of the database, the more frequently such surveillance takes place. The boundaries of the database and its usage also become a form of social differentiation between a “We, the normal, trusted citizens” and a “They, the Others, the non-trustworthy”. Who falls within this defined population that is subjected to such “bio-surveillance” (Williams and Jonson 2004a) has expanded dramatically in less than the nine years that the Norwegian DNA database has been operational. At work is a very familiar process whereby legal restrictions are loosened to be able to use a surveillance technology more (Haggerty and Ericson 2006: 19) and laws and regulations are pushed to obtain desired goals.

In Norway acquitted suspects are to be removed from the investigation-database. The UK had a similar practice until a change allowed indefinite retention of DNA samples. The background for this change was the failure to ensure systematic removal of profiles from the NDNAD of people who were never convicted. At least 50 000 profiles might have been kept unlawfully on the database before the 2001 law was changed (Her Majesty’s Inspectorate of Constabulary, 2000). Function creep may happen as a bit of administrative convenience (Surveillance Studies Network 2006), and also tends to turn up ad hoc (Haggerty and Ericson 2006). This expansion of the NDNAD may be an example of both processes. But is there a road back in time? While indefinite retention of samples was unacceptable and unlawful when the NDNAD was first implemented, objections fade as expansion occurs gradually. As one interviewed British DNA-manager said:

"I suspect -- this is my personal view -- but had they tried to bring in the current legislation back in 1995 they would never have gotten it in. It was far too radical at that point. But if you bring it in a limited fashion and say it is only for criminal elements and that proves to be extremely successful, then bit by bit you can add on to that, which I would say is probably what happened to allow us to get to this point. I do say there is probably still a good deal of controversy over keeping profiles related to people who have never been charged of anything but who were unfortunate to be in the wrong place at the wrong time, because once it is on, getting off the system is not easy. But I am quite sure this won't change."

In general, surveillance technologies have been on the rise in recent years (Innes 2001:3). DNA is seen as reliable, trustworthy and secure tool. DNA is expected to increase security on a micro and macro level; the individual's legal protection and society's rule of law (Dahl 2009). Therefore this may also be an example of how security may trump a wide range of possible counter-arguments. This is obvious in an interviewed British policeman's account of why people not convicted of crimes should go on the NDNAD:

"It's quite a harsh law to say that we would take and keep DNA from people who have never been convicted, but it has proved for us. We have evidence of hundreds of cases where DNA has been taken, that have not previously offended. They are first time offenders, who have not been convicted before. Yet their DNA is matched against very, very serious offences of rape, murder, or whatever. If we had not had this legislation, had we not had this law, to take the DNA and to retain it to check it against the database, we would have never detected those crimes. Although it could be

considered, and I can understand the argument, that it is a very harsh law, it is actually worthwhile".

An equivalent cost benefit analysis, how catching criminals and enhanced security will trump any other argument, appears in the National DNA Database Annual Report 2005-2006 (p14):

"*The Government appreciates that some people may be concerned about building a larger DNA database, particularly where it relates to people who have not been proceeded against for an offence. However, it has concluded that any intrusion on personal privacy is both necessary and proportionate, to the benefits for victims of crime and protecting the public against criminals*." [10]

Sometimes function creep takes place as new possible uses of technologies emerge that were not foreseen at the time of implementation. These often provide new consequences and risks (McCartney 2006), not properly accounted for, nor protected against. One such example with DNA is familial searching. Familial searching is based on the fact that DNA is inherited from our kin and that DNA profiles of blood related individuals are more likely to contain similarities than those of unrelated individuals. Familial searching may then provide guidance to investigations where a full DNA profile has been obtained from the crime scene sample, but where one does not obtain a match when the sample is loaded to a DNA database (McCartney 2006: 190 and Williams and Johnson 2008: 73-75). This opens not only for surveillance of convicts (or even suspects) but also their families. As this was not anticipated when forensic DNA databases were first implemented, no rules and regulations existed for it.

[10] Here we may be seeing how one notion of "risk" rhetorically contributes to security trumping privacy interests. Some outcomes are simply seen as so risky (in the sense of potentially harmful) that no calculable risk (in the statistical sense) is acceptable and no calculable "cost" (such as loss of privacy or autonomy) too great if it can bring one even marginally closer to zero risk.

Even though now well-known in the UK, in Norway even the most recent regulations still make no mention of familial searching. A Norwegian policeman said the following about this gap:

> *"As of today we do not conduct familial searches in the DNA database in Norway. But technically speaking there is no obstacle to it. Technically the database solution is arranged so that it is doable. But I guess we haven't gotten that far when it comes to the line of thought around it that it has been on the agenda in Norway yet."*

Here Norway seems to have lost a rare opportunity to regulate an activity before it becomes commonplace. This is a shame as other stakeholders claim that once a technological development has taken place it is too late to turn back. As a person from the Commission for Forensic Medicine said[11], "*That debate [about familial searching] should have been had during the early 90's or at the end of the 80's if we did not want it. But who could have seen it coming?*"[12]

An obvious challenge is to keep laws and regulations up to date with technological developments. Technological development is seen as moving at a much quicker pace than legal change. Thus "regulatory gaps" or "legal loopholes" arise. A Norwegian DNA-laboratory worker said the following about legal loopholes: *"The legislature doesn't manage to think of all the contingencies. And this isn't all that strange, but it means that there are quite some special occasions"* While another DNA-laboratory worker expressed the following about how he felt the police relate to such legal loopholes: *"they read the law the way the devil reads the bible (…) They say that that which is not explicitly claimed illegal, is*

[11] The Commission for Forensic Medicine is a national commission appointed by the Ministry of Justice. Their main task is to ensure quality of forensic medicine expert witnesses'' reports given in criminal law trials.
[12] Technology-determinist claims such as this also have a function creep-advancing rhetorical effect, but we won't discuss that further here as we have no specific suggestions as to measures to counteract them, other than simply an alert and informed public discourse.

legal". And at the same time lab staff claimed to be more or less certain that the police had cheated them at times to make them do illegal analyses, but covered in a way so that they could not really see or say they were illegal.

Regulatory gaps imply that rules and regulations may not be enough to be able to control function creep. Writing laws is a slow Parliamentary process, revising them equally slow and too rarely addressed. Sunset provisions mandate that a law will expire on a particular date, unless it is reauthorized by legislature[13]. It may be applied to an entire legislation or parts of it[14]. This is a way to make sure that legislation is reviewed and kept up to date. It is also a way of ensuring that usage does not expand uncontrolled. Even so, this is a process that happens with years in-between, and not on a day-to day basis. How then might we manage to deal with issues and conflicts arising on a day-to-day basis? We will discuss several possible channels for this below.

3.3 Ethics committee

Ethical issues that were not possible to foresee at the time of implementation are bound to arise. Rules and regulations may not cover such issues. One way of dealing with ethical issues as they arise may be to have an ethics committee to oversee the technology and its surrounding practices. Medical biobanks are subject to regulation by ethics committees. These evaluate research projects that propose to use data from the biobanks. They also evaluate data collection procedures, procedures for withdrawal of personal data, and individual cases of

[13] http://legal-dictionary.thefreedictionary.com/Sunset+provision
[14] http://www.berr.gov.uk/whatwedo/bre/policy/scrutinising-new-regulations/preparing-impact-assessments/toolkit/page44269.html. Last accessed 16.10.08

conflicts concerning biobanking practices. Additionally, ethics committees may give opinions on issues that are more a matter of principle[15].

The UK NDNAD has such a committee – the Ethics Group. The Ethics Group is relatively new (since 2007) and has so far had four meetings. From their published minutes[16] we can see that they have discussed such matters as volunteer consent, causes and implications of ethnic imbalance in the NDNAD, and routines for handling applications to conduct research on the NDNAD. It is impossible to say what effects the implementation of the Ethics Group will have, but some critical issues have already been raised. The Nuffield Report (2007) points out that the Ethics Group is not as autonomous as one might have wished. The Ethics Group is organizationally placed directly under the NDNAD Strategy Board. It is the Strategy Board that decides which research proposals will be discussed by the Ethics Group. The Strategy Board's agenda-setting power is a serious restriction on the Ethics Group's autonomy.

Another critique, not raised against the Ethics Group specifically but shedding doubts on the effects of regulatory bodies such as ethics review boards more generally, has been framed by Pfeffer (2000). Pfeffer found, in her study of the regulation of IVF services and research, that the implementation of the Voluntary Licensing Authority (VLA), rather than restricting activities, set clinics free to push the envelope. "In granting licenses and reviewing research protocols, the VLA staved off threats to outlaw human embryo research, thereby enabling scientists and clinicians to continue manipulating and sometimes destroying human embryos." (Pfeffer 2000: 265)

[15] For more on the workings of ethics committees, see http://www.etikkom.no/English
[16] http://police.homeoffice.gov.uk/operational-policing/forensic-science-regulator/about-the-regulator/ndnad-ethics-group/

We would claim that the research reflected in data-sharing requests, as have been made towards the NDNAD (GeneWatch 2006b: 2-3), could arguably be seen as function creep, since research was not one of the original intentions of the NDNAD. In establishing procedures for approving such requests, even if after an ethical review, evaluation by an ethics committee might serve not only to keep this type of function creep under control; it might also be a mechanism that allows it to take place.

Another critical issue is committees' composition. Function creep will take place because someone considers an expansion beneficial for themselves, for some social group, or for society as a whole. Having interviewed stakeholders about the matter it appears that, not surprisingly, our informants remain true to their occupational interests. For instance, a Norwegian policeman said the following regarding the ethics of familial searching:

> *"I perceive it as unproblematic to conduct familial searching if it was to become available. That is my conclusion. Because it will be a tool to bring us closer to catching the perpetrator. Then we are back to basics: to catch".*

The policeman remained true to his occupational interest, "to catch criminals". Therefore an important factor will be the composition of the ethics committee. To have relevance and credibility it should consist of people of different backgrounds, stakeholders of differing orientation towards forensic DNA questions, e.g. lawyers, privacy-advocates, researchers, ethicists.

In Norway, as of now, there is no ethics committee with the remit to oversee the usage of the forensic DNA database. It is probably just a matter of time before research requests and

requests for new forensic applications, such as those made in the UK, will turn up in Norway as well. As the laws on the matter are unclear and there is no ethics committee, the Norwegian DNA database remains vulnerable to such requests.

3.4 Control committee?

While an ethics committee would consider the ethical issues of a DNA-database with the intention of evaluating a need before it takes place, a control committee would be mandated to oversee that rules and regulations are upheld. While in Norway there is no control committee as such, in the UK there is the Custodian. The Custodian is entrusted with maintaining and safeguarding the integrity of the NDNAD and developing policy (Nuffield 2007: 93).

Pfeffer's point on the role of regulatory bodies would also apply to control committees – they might unleash functional expansion as much as rein it in. This can be an effect of externalizing responsibility for ethical and legal issues, as illustrated in the following interview excerpt. Having discussed moral issues with the interviewer, a policeman said the following:

> *"You have these big moral issues involved, but as a policeman I don't think we can go too far, as long as we are correctly marshalling ourselves, as long as someone is looking at us to make sure we are doing it right. But science will continue to grow, won't it, and will give even better results of it.* (…) *I would have an outside body; the Majesty's Inspectorate. They watch to make sure the police deal with things properly and fairly."*

This policeman, who doesn't see the possibility of the DNA database going too far, claims that there should be a control committee to keep an eye so that the police do not misuse the DNA database. At the same time, it also shows that the existence of a control committee is felt to release the policeman from the responsibility to police himself.

3.5 Sanctions

One major problem with many laws and regulatory bodies is that they are ineffective in large part because they lack sanctions. For instance, in Norway there are many rules governing the collection of forensic evidence, yet even illegally collected evidence may be permitted in court. This openness for unlawfully collected evidence also encompasses unlawful uses of DNA database information. Strandbakken, the leader of the Norwegian White Paper committee on expansion of the DNA database, writes: "Even if a DNA-stain is collected contradictory to the Criminal Procedure Act, a Norwegian court will probably not exclude the evidence" (Strandbakken 2007: 352, our translation).

There have been a number of examples where Norwegian police have used, if not illegal, then at least untraditional methods to obtain a DNA profile and search it against the DNA database. In one instance, a man the police suspected of a serious crime happened to drown, his body thereby arriving at the Institute of Forensic Medicine for an autopsy. This was very convenient for the police who, without asking consent of the next of kin, took a sample for comparison. This sample exonerated the man, but implicated his brother through familial similarities. Another suspect in the same case died of cancer. Here the police requested access to tissue samples at the hospital but were turned down. The case went all the way to the Supreme Court, which ruled against the police request. This Supreme Court ruling casts the use of the drowning victim's DNA in a critical light, but did not prevent the use of the

evidence in court. Other creative collection methods have also been used. In one case police picked up cigarette butts from a person's garden. In another a suspect was called in for questioning on an unrelated case, one in which he was not a suspect but a witness. In this relaxed atmosphere he was served a glass of water which then was used to obtain his DNA profile for use in the case in which he was a suspect (Strandbakken 2007). Such creative, and some would say illegal, ways of working have however no formal consequences for the police.

It is important that sanctions are clear and effective. Additionally, it should also be possible to apply these sanctions to both individuals and organizations that are caught misusing data.

3.6 PETs

Even the most effective sanctions, however, primarily come into play after a breach has taken place. Before that, they have only a presumed or hoped-for cautionary effect. Another way to back up intentions with enforcement is to inscribe (Akrich 1992) the enforcement directly into the technology. In the case of DNA databases, privacy-enhancing technologies (PETs) might be built into the database software.

For instance, in Norway suspects are first entered into an interim suspect database. If convicted, their profiles are moved to the permanent database. The Liberal party has proposed that juvenile offenders should be taken back off the permanent database if they are not convicted of another offence within a certain amount of time. This removal of first time offenders could be automated within the data program.

There is some legal precedence for demanding the inclusion of PETs within database software. In a recent case -- *I v Finland*[17] -- the European Court of Human Rights (ECHR) points to the state's responsibility to implement effective measures to preserve citizens privacy. The state is not only required to punish unauthorized access, or offer compensation for injuries as a result of unauthorized access. "What is required in this connection is practical and effective protection to exclude any possibility of unauthorized access occurring in the first place".[18] For the health sector, as this case was based on, this implies effective measures within the technical systems to protect a patient's privacy.

Of course, just as with the legal and organizational measures proposed above, PETs are not in themselves a sufficient guarantee against unwanted function creep. PETs are a "technological fix". Technological fixes can be worked around by the technologically competent, while they are incomprehensible to most of us, leaving us to either trust or distrust them blindly. Therefore they should always be part of a larger package of measures (McCarthy 2008).

3.7. Transparency

So far we have discussed measures that imply the state watching and controlling itself. However, it is a democratic state's duty to provide transparency so as to enable the possibility of *sousveillance* (Mann 2002). Sousveillance describes situations where the public watches and thereby controls the state by opening up for the possibility to comment and/or object to observed practices. Of course, when it comes to forensic technologies, transparency runs up against the perceived necessity that police methods be kept secret so as to prevent, or at least

[17] Application no 20511/03, Judgment of 17 July 2008.
[18] *I v Finland*, Paragraph 47

delay, criminal elements in finding ways to evade them. The problem of transparency becomes particularly fraught in connection with data-sharing.

Function creep on DNA databases may take place because new technologies permit increasing amounts of data exchange. With such exchange the question of who may have access to the information of the DNA database becomes murky. Rules and practices change as geographical and organizational distance between practitioners and stakeholders grows, and transparency may suffer. To illustrate this regarding forensic DNA databases, we will use the Prüm Treaty as an example.

The Prüm Treaty is the first international treaty which arranges an automated cross-border matching of biometric data.

> *"Prüm, also known as Schengen III, does not only govern the automated searching and comparison of police DNA databases for the purpose of criminal investigation, but the automated searching of fingerprint data and national vehicle registration data for preventive purposes and, in the case of vehicle data, even to track administrative offences. Moreover, the Treaty sets out the framework for information exchange to prevent 'terrorist crime' and cross-border police operations such as joint patrols and administrative assistance in case of major events or natural disasters"* (Töpfer 2008: 14).

The Norwegian Minister of Justice, who is currently (September 2008) applying for Norwegian membership in the Prüm Treaty, justifies this function creep as follows:

> "*Through the DNA-reform and probably Norwegian affiliation to the EU-countries DNA-databases through the Prüm Treaty, the government is taking a large step*

forward in the fight against the internationally branched crime. This is quite necessary. We have to build up under international co-operation that will enable us to deal with globalised crime (…) We have to show that politics is to be willing, also outside the countries borders (…) The development of global trans-boundary crime requires this from us".[19]

If Norway is accepted as a member of the Prüm Treaty the use of DNA profiles which were given before membership of the treaty was in place will be under the same scrutiny as profiles registered after membership, changing what manipulations may be performed on the materials and thus changing the "deal" between the registered and the database owner:

"*Although the treaty stipulates that database access has to be log-filed and follow defined purposes, the automated cross-border exchange of police data is only limited by national legal protections, and these differ regarding data protection standards and the regulation of DNA analysis and DNA databases."* (Töpfer 2008: 14).

In other words, data are managed according to the laws of the country where the data are at any given moment. Data used in Norway may have been collected according to laws from elsewhere; data gathered in Norway may wind up being stored and used elsewhere according to laws Norwegians have little knowledge of or influence over. Note that in the case of forensic DNA databases, there is nothing that the registered may do if they disagree with the changes. This as opposed to medical databases that are dependent on people's willingness to contribute samples for both research and storage (Kettis-Lindblad et al 2005: 433) and where

19

"http://www.regjeringen.no/nb/dep/jd/dep/Justisminister_Knut_Storberget/taler_artikler/2008/grenselos-kriminalitet.html?id=522615 (our translation)

people may withdraw their samples if they disagree with what is taking place. This is due to the fact that samples are "given" by medical "donors" but "taken" from "suspects". These differences influence how consent, privacy, and autonomy, are presented in the two contexts (Johnson and Williams 2004b: 211). Nevertheless, even though "participation" is non-voluntary – or perhaps all the more so when participation is non-voluntary – issues of trust and transparency become important in relationship to forensic DNA databases: "It is often asserted that the maintenance of public confidence, or trust, in the operation of forensic as well as medical databases is partly dependent on the openness and transparency of their operation" (Williams and Johnson 2008: 139). Because the power balance between the registered and the owner of the DNA database is not equal, there is a need for the possibility of public debate about the uses of forensic DNA databases. This requires transparency. Proposed new functions should be widely publicized and accepted by the public before being irredeemably entrenched. It would be important that such reports account for not only what has happened in certain high profile cases, but also account for procedures that are used, reporting achievements, possible changes in rules and regulations, what new measures may be achieved due to technological development, what kind of ethical dilemmas that have arisen etc. A British interviewed policeman said the following:

> *"The fear is the lack of understanding of what the DNA database does now and how the DNA database works. And so to allay those fears you've got to make it very public about how you are going to use it. And it's got to be very transparent, so people can be reassured that it is used properly, ethically and in line of what it was designed for."*

UK is attempting transparency when they provide their DNA reports. However it was only recently (in 2003) that the first publicly available document was published addressing these

issues in relation to the NDNAD (Williams and Johnson 2008: 139). In Norway, so far, no such attempts have been made. An interviewed Norwegian policeman, confronted with this situation, said, *"There you are onto something important."* However, he also expressed being skeptical towards doing too much of it: If one started doing this for DNA there might be a transparency function creep and they would have to do it for other policing techniques as well, and that might be a difficult one to balance. What has to be kept secret of police working methods and how much does the public need to know? That part of police methods should be kept secret, however, is not a reason not to publish how the DNA database is being used and with what results. "Where public access is denied for reasons of security and the administration of justice, this should be fully explained and justified." (Nuffield 2007: 106)

While the Norwegian system has not implemented practices for reporting usage and achievements, the process of expanding the forensic DNA database in 2008 was indeed transparent. This is largely due to the Instructions for Official Studies and Reports mentioned earlier. In July 2004 the government appointed a committee to consider changes to the Norwegian forensic DNA database. A year and a half later this committee delivered a White Paper (NOU, 2005:19) discussing a number of issues related to the use of DNA databases in criminal law administration, and urging a substantial expansion of the Norwegian forensic DNA database. The White Paper was then sent out for consultation to over 50 government offices, NGOs and institutions deemed likely to have relevant input on this issue. These responded with statements in which they accounted for their opinions on the White Paper and its recommendations. Highlights from the approximately 35 statements the ministry deemed most important were published (Ot. Prp. Nr. 19). In addition, the Parliamentary Standing Committee on Justice provided a document with its own views on the issue of an expanded forensic DNA database (Inst. O. nr 23, 2007). The White Paper, the responses to it and the

Standing Committee on Justice document collectively form the background material for national debates, for instance in the mass media.

3.8. Limit the potential for function creep – limit database scope

Whereas some of the safeguards we have discussed above would perhaps be useful for several forensic databases, or even for technologies in general, there are aspects of DNA that may make it require further, more technology-specific safeguards in relation to function creep. DNA possesses properties that may raise further ethical and social concerns than do other identification databases or criminal registers. Here we think it is crucial to differentiate between the storage of DNA samples and DNA profiles.

A DNA sample is the biological material gathered to determine the identity of the person registered, today typically a mouth swab containing cells from an oral cavity. By conducting analysis on selected segments of the chromosomes, a DNA profile is obtained. A DNA profile is a string of numbers and/or a graphic print of patterns in our DNA. A DNA sample on the other hand is part of our body and it is "entirely possible to sequence a part or all of an individual's entire genome from their biological sample, and therefore, the retention of biological samples requires much greater critical attention and justification" (Nuffield 2007: 54). Aspelenn and Lane (2006:1) claim the uses to which samples can be put subsequent to a usable database profile being developed are rarely specifically regulated. This may be due to the fact that countries generally fail to identify possible future uses of biological material.

Function creep has already taken its first, but probably not last, step in relation to research on DNA databases: According to Genewatch (2006a:8) research has already taken place on the NDNAD. This research has ranged from studying the efficiency of the database and the

validity of its statistics to developing new commercial products. Research has used both the DNA profiles from the database and the stored DNA samples. Obviously this is an extension of the use of the NDNAD. The notion of function creep on biological samples was discussed in Odelstinget, as witness the question and answer quoted below from members of the Standing Committee on Justice:

> ***"Ingrid Heggø (Labour Party): O****ne of the main reasons that we don't think the biological samples should be retained is that we are afraid they will be used for research in the future. When we have such a large database over convicted criminals somebody may get tempted to conduct research on them to see if they can find a common thing that characterizes a criminal, for example a murderer.*
> *What is Fremskrittspartiets (Progress Party's[20]) view on such research today? If they are against, why should we believe that they won't turn around in a little while in this case, like they most often do in other cases?*
>
> ***Solveig Horne (Progress Party)****: We have an amendment of a law up for hearing today where considerations are being made as to whether research should be permitted or not. The Progress Party clearly agrees with the proposal that is being discussed here today. We are not going to change anything in this round, and we have not been given a message from the cabinet minister that there will come a new amendment of the law the next years when it comes to this case."*

The introduction made by Heggø illustrates some of the rationale from politicians' views for not retaining samples. Retention of samples requires that we not only trust the government

[20] A right-wing populist party most known for being against taxes and for restrictions on immigration.

today, but also that of tomorrow (since we do not know what will be doable with the genetic material in the future). The possibility of data-sharing across borders requires further that we trust other governments over whom we hold no democratic sway.

We also see how Horne evades the actual question. She is in no position, nor would representatives for any other party be in a position, to make a definitive promise. No party can guarantee that they will never accept function creep. This may be one of the reasons why the Norwegian Parliament went against what was recommended to them by the DNA-committee, and voted against retention of samples. Short of not collecting DNA in the first place, the most effective way of limiting research on DNA gathered for forensic uses is to destroy samples and only retain profiles. This is also a more permanent way to protect privacy (Steinhardt 2004: 190). Limiting the scope of the database in this way implements "brakes" and safeguards, allowing more time to reflect what direction it is desirable to move in the future. Research will still be possible, just more expensive and laborious as new samples may have to be gathered.

Returning to our earlier point about interpretative flexibility being a basic premise for function creep: Information is almost limitlessly interpretatively flexible; databases almost limitlessly searchable and analyzable. Thus, the best way to limit the function creep of information databases is to limit the information they contain.

4. Is there a moral to this story?

Function creep seems nearly always to take place on surveillance technologies, and as we have shown in this article forensic DNA databases are no exception. When additional

functions are added to a technology slowly, people will often be less skeptical of the development than they might have been had those functions been proposed early on. We can already see that our resolve against expanding uses for DNA-technology has been weakened. When it is used for one purpose, then another, why should a third matter? "As Marx warns: "Once DNA analysis comes to be seen as a familiar and benign crime control tactic, the way will be paved for more controversial uses" (Marx 1998).

While forensic DNA databases and function creep on them may contribute to increased security, they may also contribute to increased *in*security. Often it comes down to a value judgment whether a given function expansion is considered positive or negative. In this article, drawing on data from a larger project, we have shown some examples of function creep. Looking to the past, present and future we have presented some safeguards that we believe should be in place to enable the governing of forensic DNA database functions and practices. Clearly none of these safeguards are sufficient on their own; they need to work together.

In the UK safeguards in relation to the NDNAD have been developed over the last 13 years, and are still being developed. Norway's DNA database has a slightly shorter history and is far less extensive than the English and Welsh NDNAD, but this is not due to safeguards already in place. Instead we see that the safeguards too seem to have developed at a slower pace than in the UK. Without effective safeguards in place, we can look to UK practices and see our future virtually inscribed … some of it promising, and some of it alarming. Using what safeguards we do have available, it is now up to us to mobilize the forces of democratic debate.

Not only do we need debate; we need that debate to achieve some level of sophistication. "[W]hile the technology is still undergoing development, the sophistication of ethical and normative debates have not advanced at a similar pace, leaving issues of human rights and civil liberties still to be properly accounted for" (McCartney 2006: 193). In current debate we see that the rhetoric supporting crime prevention initiatives, including function creep on existing systems, is often expressed in binary opposites: safety vs. privacy, or security vs. rule of law, or suspects' rights vs. victims' rights (Dahl and Lomell forthcoming). In this article we have seen how arguments such as crime prevention, security and safety have trumped ethics and human rights issues such as privacy, rule of law and freedom.

Expansion of DNA databases challenges human rights such as the presumption of innocence, because the very structure of standard database usage procedures implies that earlier criminals are considered probable suspects of future crimes and must "prove" their innocence by not matching crime scene samples. Specific DNA database usages entail further ethical challenges. Familial searching, for instance, may confront citizens, with previously unknown family ties. The use of ethnic inference borders on the ethically dubious practice of racial targeting.

McCartney seems pessimistic as to the ability of human societies to rise to these challenges. "The protection of the public in risk-averse society will always trump individual rights" (McCartney 2006: 196). Always? Perhaps. Perhaps social discourse will always fail to recognize dangers to human rights, will always slip into a comfortably distanced vision in which those dangers only affect the "Others" (i.e. criminals) and never ourselves. So perhaps we are being naïve in writing this article, yet it remains our hope that it may help spark a more reflective and balanced debate.

References

Aas, K F, Gundhus H O and Mork H L (2009) ”Introduction – Technologies of (in)security in K F Aas, H O Gundhus og H M Lomell (ed.) *Technologies of Insecurities. The Surveillance of Everyday Life* London: Routledge-Cavendish

Akrich, M (1992) The De-Scription of Technical Objects” in Bijker & Law (eds.) *Shaping Technology/ Building Society. Studies in Sociotechnical Change*. Cambridge, MA: MIT Press: 205-224.

Aspelen, C H and S A Lane (2006) The NON-Forensic Use of Biological Samples Taken for Forensic Purposes: An International Perspective.

http://aslme.org/dna_04/spec_reports/asplen_non_forensic.pdf

Bijker, W E (1995) *Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change*. Cambridge: MIT Press.

Bijker, Wiebe E (1996) Democratization of Technology – Who are the Experts? Posted in The World Series on Culture and Technology, http://www.angelfire.com/la/esst/bijker.html, last accessed 22 Sept 2008

Bræk, R et al (1982) *Håndbok i systemarbeid* [Handbook of System Engineering] Trondheim: Tapir

Collin, H and T Pinch (1994) *The Golem – what everyone should know about science* Cambridge: Cambridge University Press

Dahl, J Y (2009) Another side of the story: lawyer’s views on DNA as evidence in K F Aas, H O Gundhus and H M Lomell (ed.) *Technologies of Insecurities. The Surveillance of Everyday Life* London: Routledge-Cavendish pp 219-237

Dahl, J Y and H M Lomell (forthcoming) Tallenes tale: Bruk av statistikk i legitimeringen av kriminalpolitiske tiltak (Numberspeak: The usage of statistics in crime policy legitimation processes)

Fox, R (2001) "Someone to watch over us: Back to the panopticon?" *Criminal Juatice* 1 (3) pp 251-276

Garland, D (1995) Panopticon Days: Surveillance and Society *Criminal Justice Matters* 20 (1) pp 3-4

GeneWatch (2006a) The DNA Expansion Programme: reporting real achievements http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/DNAexpansion_brief_final.pdf

GeneWatch (2006b) Using the police National DNA database – under adequate control? http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/research_brief_fin.doc

Haggerty, K (2009) "Ten Thousand Times Larger…: Anticipating the Expansion of Surveillance" in D Neyland and B Goold (eds) *New Directions in Privacy and Surveillance* pp. 159-177 Cullompton: Willan Publishing

Haggerty, K and R Ericson (2006) *The New Politics of Surveillance and Visibility* Toronto: University of Toronto Press

Her Majesty's Inspectorate of Constabulary (2000) *Under the Microscope* London: Her Majesty's Inspectorate of Constabulary

Hoffmann, B (2005) Er bredt samtykke i medisinsk forskning mulig og nødvendig? [Is broad consent in medical research possible and necessary?] *Tidsskrift for norsk lægeforening* vol 17

Home Office (2006) The National DNA Database Annual Report 2005-2006 London: HMSO

http://cmiskp.echr.coe.int/tkp197/view.asp?item=14&portal=hbkm&action=html&highlight=Application%20%7C%20no%20%7C%2020511/03%2C%20%7C%20Judgment%20%7C%2

0of%20%7C%2017%20%7C%20July%20%7C%202008.&sessionid=14799023&skin=hudoc-en

I v Finland Application no 20511/03, Judgment of 17 July 2008.

Innes, M (2001) Control creep. *Sociological Research Online* 6 (3)

Inst. O. nr 23 (2007-2008) Innstilling til Odelstinget fra justiskomiteen [Proposal document to the Odelsting from the Standing Committee on Justice] Oslo: Ministry of Justice and the Police

Instructions for Official Studies and Reports (2005) http://www.regjeringen.no/upload/FAD/Vedlegg/Statsforvaltning/Utredningsinstruksen_eng.pdf

Johnson, P and R Williams (2007) European securitization and biometric identification: the uses of genetic profiling. *Annals of the Italian National Institute of Health* **43**(1): 36-43.

Kettis-Lindblad, Å et al (2005) Genetic research and donation of tissue samples to biobanks. What do potential sample donors in the Swedish general public think? *European research on public health* 16 (4) pp 433-440

Kranzberg, M (1986) Technology and History: 'Kranzberg's Laws', in *Technology and Culture* 27 (3) pp 544-560

Mann, S (2002) "Sousveillance" web-published article: http://wearcam.org/sousveillance.htm

Marx, G (1988) *Undercover: Police Surveillance in America* Berkley: University Press

Marx, G (1998) "DNA Fingerprints may one day be our national ID card" *Wall Street journal* 20 April

Marx, G (2005) Seeing Hazily (But Not Darkly) Through the Lens: Some Recent Empirical Studies of Surveillance Technologies, in *Law and Social Inquiry* 30 (2) pp 339-399

Matheisen, W (2001) *Samfunnsliv* Oslo: Universitetsforlaget

McCarthy, P (2008) *Privacy Enhancing Technologies – Protecting my DNA/identity? Building Trusted Citizens and Citizen's Trust* Paper presented at "Genetic Suspects: Emerging Forensic Uses of Genomic Technologies" ESRC Genomics Forum, University of Edinburgh, 2-3 October, 2008

McCartney, C (2006) *Forensic Identification and Criminal Justice – Forensic science, justice and risk* Cullompton: Willan Publishing

Merton, R K (1942) Priorities in Scientific Discovery: A Chapter in the Sociology of Science *American Sociological Review* 22 pp 635.659

Ministry of Justice and Police (2007) Auka bruk av DNA for å oppklare meir [Increased use of DNA to detect more]. Press release

NOU 1993: 31 *DNA-analyser i straffesaker* [DNA-analysis in criminal justice cases] Oslo: Ministry of Justice and Police

Nuffield Council on Bioethics (2007) *The forensic use of bioinformation: ethical issues* Cambridge: Cambridge Publishers Ltd

Ot. Prp. Nr. 19 (2006-2007) Om lov om endringer i straffeprosessloven (utvidelse av DNA-registeret) [About changes of laws in the criminal procedure (expansion of the DNA database)] Oslo: Ministry of Justice and the Police

NOU 2005:19 Lov om DNA-register til bruk i strafferettspleien [Law about DNA database for use in the criminal law administration] Oslo: Ministry of Justice and the Police.

Oudshoorn, N and T Pinch (2003) How Users and Non-Users Matter, in N Oudshoorn and T Pinch (eds) *How Users Matter. The Co-Construction of Users and Technologies*, Cambridge MA: MIT Press, pp 1-25

Riksadvokaten (2008) Letter dated 15. Aug 2008, archived as: Ra 07-569 KHK/jaa 624.7, titled: Nye retningslinjer for registering i DNA-registeret og innsamling av spor med DNA-analyse mv. [New regulations for registration in the DNA-register and collection of traces for

DNA-analysis etc.] http://www.riksadvokaten.no/ra/ra.php?artikkelid=194 (last accessed 16.10.08)

Steinhardt, B (2004) Privacy and Forensic DNA Data Banks in Lazer, D (ed) *DNA and the Criminal Justice System.* Massachusetts: MIT Press

Storberet, K (23.10.2007) "Vi skal oppklare mer" [We are going to detect more] *Østlendingen*

Strandbakken, A (2007) Innhenting av DNA-bevis — helliger målet ethvert middel? [Collection of DNA-evidence – Do the ends justify all means?] In *Jurist uden omsvøb. Festskrift til Gorm Toftegaard Nielse.* København: Christian Ejlers`forlag pp 337-354

Surveillance Studies Network (2006) *A Report on the Surveillance Society*. London: Office of the Information Commissioner. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf (last accessed 22 Sept 2008)

Töpfer, E (2008) Searching for needles in an ever growing haystack: Cross-boarder DNA data exchange in the wake of the Prüm Treaty *Statewatch* 18 (3)

Webster's Encyclopedic Unabridged Dictionary of the English Language (1994), New York: Gramercy Books.

Williams, R and P Johnson (2004a) Circuits of Surveillance. *Surveillance and Society* 2 (1) pp 1-14.

Williams, R and P Johnson (2004b) Wonderment and Dread: Representations of DNA in Ethical Disputes about Forensic DNA Databases. *New Genetics and Society* 23 (2) pp 205-223

Williams, R and p Johnson (2005) *Forensic DNA Databasing: A European Perspective* Interim Report. http://www.dur.ac.uk/resources/sass/WilliamsandJohnsonInterimReport2005-1.pdf

Williams, R and P Johnson (2008) *Genetic Policing: The Use of DNA in Criminal Investigations*. London: Willan Publishing.

Yuthas, K and J F Dillard (1999) Ethical Development of Advanced Technology: A Postmodern Stakeholder Perspective *Journal of Business Ethics* 19 (1) pp 35-49

Zedner, L (2009) "Epilogue: the inescapable insecurity of security technologies?" in (eds) K F Aas, H O Gundhus and H M Lomell *Technologies of Insecurity* London: Routledge Cavendish