Identifying Legal Concerns in the Biometric Context

Yue Liu
Norwegian Research Centre for Computers and Law
Faculty of Law
University of Oslo

Abstract: This paper aims to contribute to the debate of biometrics and privacy concerns by examining the existing legal and academic debates. Several controversial legal problems in the biometric context will be discussed such as the following: the legal status of biometric data, the storage of biometric data, compulsory and voluntary issues and the necessity of using biometric technology. The study will be based on relevant EU instruments, Norwegian, Swedish and US case law. Critical comments will be made on the various views about biometrics and data protection from a legal perspective.

Key words: biometrics, data protection, privacy, identification, authentication

1. Introduction

Biometric-based personal verification or identification systems (Wayman, J. L 2000) that use physiological or behavioural trait are becoming increasingly popular, with the unprecedented rate of recent advances in information technologies (Wayman, J. L.2000 and Miller, B. 1988). Commercial and government entities are the two main forces that embrace the technology. Japanese cell phone manufacturers have begun including fingerprint readers into their devices to prevent unauthorised use (Phred, D. 2004). Biometric payment systems using finger scanning technology are now in wide use in American chain stores. (Rinehart, G. 2006) Norway and Sweden became the second and the third countries in Europe to introduce biometric passports using facial recognition and the RFID chips. More and more people are obliged to accept the biometric technology as an authentication method without really understanding or thinking about the consequences. Both technicians and legal professionals are still concerned about the permissibility of using biometrics on a large scale, especially from a privacy perspective.(Johnson , M.L.2004 and Ashbourn, J.2004) Understanding the law and policy concerns is therefore necessary for both technicians and lay people. This new technology is sparking new laws and causing old legal doctrines to be revaluated and reapplied by the nation's law and policy makers.

The use of biometric technology as a key component of an overall strategy to improve national security and reduce fraud has been adopted by several legislative and regulatory initiatives. The new technological reality of biometrics has forced us to explore further what is required for safeguarding the basic human rights of privacy and to ensure the optimal results for society. Given that there are many conceivable biometric applications, it is true that "whether the use of biometrics gives rise to additional risks or provides better protection and more privacy depends on the specific application" (Grijpink, J. 2001) However it is also true that without strict legal regulations it is unlikely that adequate concerns about privacy will be addressed when adopting the biometric applications.

This paper aims to contribute to the debate by examining the law and policy concerns of biometric applications from a privacy perspective. The legal concerns being touched upon in this short paper are by no means exhaustive. Through the analysis and discussion of the various legal initiatives or arguments in the biometric context, hopefully it will be able to give a hint of the complexities involved in biometric technology by focusing on several controversial legal issues.

2. Legal status of biometric data

The legal significance of biometric data, including raw biometric images and biometric templates, has been discussed by many legal and non legal professionals. Although there were different views about whether a biometric template should be regarded as personal data, or personal related data (Grijpink, J. 2001), or anonymous data (Prins, C.1998), there is no denying that raw biometric data is personal data in the sense of the EU directive. In the report to the European Commission, Paul de Hert (2005) had given a clear clarification as to why a biometric template should also be regarded as personal data. [1] It will be tedious to repeat it here as basically we

[1] The Directive equates 'personal data' with any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Raw

have similar arguments. Hence the starting point of our discussion is biometric data including raw image and templates, should be regarded as personal data covered by the Data Protection Directive.

2.1. Is biometric data sensitive personal data?

A question which has not received enough analysis is when should biometric data be regarded as sensitive personal data? Corien Prins (1998) claimed that "in certain situations the use of biometrical data could imply use of sensitive personal data". The question is then, in what situations would this arise?

Article 8 of the Directive states that processing of "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life" should receive "explicit consent" of the data subjects unless in certain listed circumstances. It indicates that personal data, which can reveal the above listed information, should be regarded as sensitive personal data. The data protection working party held that some biometric data could be considered as sensitive in the meaning of Article 8 of Directive 95/46/EC, when it reveals racial or ethnic origin or data concerning health. But whether a processing contains sensitive data is a question of appreciation which can only be determined by specific biometric characteristics used in the biometric application itself. (Data Protection Working Party , 2006) They proceeded to give the example of facial image as obvious sensitive data and then stopped to give any further clarification. What are the specific criteria for determining the sensitiveness of biometric data? When exactly should it be regarded as "reveals racial or ethnic origin or data concerning health"? The guidance here is nebulous. It may be tempting as the working party suggested, to leave the freedom of appreciation to judges for deciding whether the biometric data being used is sensitive or not. However as the technology develops, this suggestion does not seem to be so appropriate, especially when taking into account that the understanding of the biometric technology among people, including judges other than scientific experts, is still quite limited.

One of the most prevalent privacy concerns about biometric data is based on the fact that biometric data is disproportionate to the task at hand. A single piece of biometric data often consists of two categories of information: information usable for authentication and information not usable for authentication. Information usable for authentication includes information such as: Genotypic information, Randotypic information (sometimes called phenotypic, but without genetic parts), Behavioural information, Information about "unchanging marks". (Bromba.M, 2003) Genotypic information is completely determined by genetics. With respect to data protection, genotypic information seems to be the most controversial since it might reveal relationships to other persons, race, or even a potential disease. For instance, Dr. Marvin M. Schuster has discovered a "mysterious relationship" between an uncommon fingerprint pattern, known as a digital arch, and a medical disorder called CIP. Based on a 7 year study, he found that 54 percent of CIP patients have this rare digital arch fingerprint pattern. (Hancock, E. and Hendricks, M 1996) While still controversial within the scientific community, several researchers have reported a link between fingerprints and homosexuality. (Cytowix, R.E. 1996)

Randotypic information is completely random, and behavioural information is completely determined by training. Unchanging marks may be scars, tattoos, or a chronic disease. (Bromba, M.2003) Among these, "genotypic information" and "unchanging marks" can be relevant to racial, ethic or health information. Information about a chronic disease will also be included because permanence is one of the basic characteristics of biometric information. Information not usable for authentication may include an acute disease. Although at present not all biometric data has been reported to be able to reveal sensitive information, the basic components of biometric information indicate unlimited potential possibilities. It is reasonable to infer as science develops, more sensitive information will be disclosed by the application of biometric information, by a fast analysis of technique equipment and this information may or may not be relevant, for the purpose the data has been collected.

How about the biometric template then? There are two possible ways that one may trace sensitive information from the biometric template: first, trace the raw biometric data from biometric template; second get sensitive information directly from the template. So are they technically possible? The possibility of reconstructing raw data from the biometric template has been discussed by many scientific experts. Suppose some relevant information is available, it has been proven that it is indeed possible to reconstruct those parts of the raw data information which is used for authentication. (Soutar, C 2002) Such data, as analysed above, may include sensitive information, so the biometric template actually includes relevant sensitive information. The second possibility of using the biometric template directly, to trace the sensitive information has not been discussed so far as the author has been able to discern, while it has been discussed as a security issue by some researchers. (Bromba, M 2003) Hence, it will be premature to make an assumption so early, without consulting scientific expertise. The progress report of convention 108 by the Consulting Committee(Consultative Committee 2005) states: "the choice of data

---

biometrical images of a person, including templates derived from raw biometrical images, are personal data in the sense of the Directive.

be extracted in generating a template should avoid revealing sensitive data as, in general, these data will not be able to verify the data subject's identity or identify him or her." This requirement seems to be contradictory to the above analysis as it indicates that the Consulting Committee considered it possible to separate the "sensitive part" of biometric data from the part used for "extracting template" which is aimed for verification or identification. However, according to our above analysis, the so called "sensitive information" is included in the "information useful for authentication"; therefore it would be difficult to exclude them out.

As we have established there is some link with health information and biometric information either in raw data or in the biometric template. Should it be safe to conclude that they are sensitive? The idea of treating the biometric information as sensitive information in general has not received much support. The concern here is that biometric information *per-se* is not directly disclosing the health information and it would take a significant technological shift to go from current biometric systems to systems that reveal disease or other health information. Furthermore, at present only some of the biometric information such as fingerprint, Iris, DNA has been proven to be able to disclose health related information. It might be relevant to mention the interesting case decided by the Norwegian Data Protection Authority concerning STVC-footage (fjernsynsovervåking) inside buses and railways. It concluded that the holding of the mere footages (lagrete kameraopptak) are not to be considered as personal information (personopplysninger); only when somebody is about to process footage to identify some criminal offender, will this processing amount to personal information. (Datatilsynet, 2004) The decision is based on the idea that the footage itself , like a blood sample, (Bygarve, A.L.2003) before analysis or using certain equipment cannot be regarded as "identifiable", as it is the "carrier" of the personal information, not the personal information itself directly. By the same token it might be reasonable to conclude that biometric information per se may not be regarded as sensitive information, unless some measures are intended to be adopted or have been adopted to use the biometric information to disclose health or genetic information.

This argument may make sense in theory; however, it remains to be seen for its practical value. To some extent it may restrict the private data controllers from using the biometric information to generate health or racial information without explicit consent from the data subjects, while somehow restrict the "function creep". Nevertheless, problems may still exist as it may be more practical and likely the commercial entities or public sectors not really need to generate such information *from* the biometric information, but simply use it as a unique, popular and convenient key data to get such information directly. This is what has been high lighted as the potential *linking and tracking* ability of biometric data. However, this nature may arguably make biometric data *sensitive data* in general. As Jon Bing (1972) pointed out in his classic paper on the classification of personal information:

> Certain key data (especially the personal number) are not sensitive per se, but derive sensitivity from the information to which one gains access through the key. This means that, in order to determine the sensitivity of key data, it is not sufficient to consider the grading this data element has been give isolated; one must also take into account what information one thereby may connect to the nexus-person. This may provide a basis for data security deliberation-the submission of the key represents in itself a threat to the protection of highly sensitive information, an increased risk of undesired access to personal information. (Bing, 1972)

Even if the health and genetic related nature of biometric data are disregarded, biometric data still distinct themselves from other common personal data by their potential abilities to be the "key data". Moreover, these key data are unlike "personal number" or other identification numbers, as they are not restricted by national jurisdictions or certain groups, they are numbers that are used around the world, especially when considering the possibility of realising general interoperability of biometric data in the future. This opinion has been adopted in the court decision of *Perkey v. Department of Motor Vehicles* (42 Cal. 3d 185, 187-8 (1986)) in the States in which fingerprint is considered as a kind of "sensitive personal information". Although in the US legal context, the "sensitive personal information" may have slightly different legal meaning from its European counterparts, the court's recognition of its sensitiveness compare with name or address may still be of some value here. So several issues arise: is it sufficient to protect biometric information as sensitive information only when it is obviously disclosing racial or health information? Will it be more preferable to regard biometric information as a new category of sensitive data? Should the list in the Directive article 8 be extended or should an alternative approach be adopted?

According to an interesting survey conducted in the UK 2006 regarding the concept of sensitive data, up to 63% respondents considered biometric data as sensitive personal data, and more than one third of respondents rated biometric, genetic and contact details as extremely sensitive, whereas only one fifth of respondents rated data concerning race or ethic origin, political opinions or data concerning religious or philosophical beliefs as extremely sensitive. (ICO, 2006) It is suggested that the time is ripe to review the provisions of the directive, in the 21 century new concerns are arising due to technological developments. (Cullagh, 2007) Considering the special characteristics of biometric data: first they are health and genetic related, second they can be used as relative

unique and universal "key data" fro getting all kinds of personal information, they should be considered as "sensitive personal data" in general, not only just when it is regarded as health data or racial data.

In concurrence with Simitis (1973 cited in Bygrave 2002), sensitively of data various from context to context, a decision to simply include a new category of sensitive data may not be taken lightly. Wacks (1989) and Wong (2007) state that what changes from context to context is not the degree of sensitivity of information, but the extent to which one is prepared or required to allow it to be disclosed or used. However categorization of sensitive data may still be understood as an indicative flexible, reference list. In practice, the list of sensitive data may be easier to restrict and protect than the "context", for example the usage and purpose need more effort to decide and detect before hand. The sensitive personal data list should become a non-exhaustive list, so as to add the biometric and other data that appear to be sensitive with technology development.

2.2. Can biometric data be anonymized and excluded from data protection constraints?

Is it possible to use biometric data anonymously in certain applications, and therefore exclude them out of the data protection constraint? Anonymity is a relative concept; as there is no absolute anonymity especially when biometric information is used. (Nicoll, J.E.J. and Prins, M.J.2003) It has been argued that when biometric information is used for verification, stored in an offline situation, for example: smart card, or local database, and without any additional identifiable information such as names, or addresses, it can be regarded as truly anonymous. Therefore it is safe to exclude it from the constraint set by the data protection legislation. (Grijpink, J.2001)

> Anonymisation is seen as particularly beneficial when processing sensitive personal data. The Directive 95/46/EC also made a specific reference to the logical exemption of anonymised data from the scope of the provisions:
>
> > …Whereas the principle of protection shall not apply to data rendered anonymous in such a way that data subject is no longer identifiable;

This is the legal basis of Grijpink's arguments. Nevertheless, it is critical to point out these arguments are also based on his other argument that the "biometric template without anything in common with the source, cannot be regarded as a personal detail because it cannot be traced back to the person from whom the measured value originated, or it can only be done with disproportionate effort." (Grijpink, 2001) This then seems to contradict the Hert's report.

We have agreed that biometric template is also personal data, as "an identifiable person is one who can be identified directly or indirectly, in particular to his physical, physiological, mental, economic, cultural or social identity." And "it is not necessary to know the name of the person to speak of 'personal data' in the sense of Directive".(Blas, D.A.2005) In the preparatory works for the Data Protection Directive, the European Commission stated that the term "personal data" should be "as general as possible, so as to include all information concerning an identifiable individual" and they also added that "the definition of personal data would also cover data such as appearance, voice, fingerprints, or genetic characteristics."(Commission 1992) Grijpink gave an interesting example comparing the fingerprint on the glass in the restaurant which is anonymous, to the biometric template without any other sources. But actually they are different because a fingerprint saved in the digitized form in the computer, is much easier to be preserved and reused. It will not really cost much effort to identify the data, since (unlike normal medical information), biometric data is created to identify people just as it was claimed in the progress report that "with regard to biometric data the option of making the data anonymous is not available as biometric data by their very nature, form an instrument to identify individuals, particularly when they are automatically processed."

Additionally, it is be relevant to mention the discussion in the UK case *R vDepartment of Health, ex parte Source Informatics Ltd.* ([2000] 1 All ER786) There it was argued that the definition of "processing" under the Directive encompasses the process of anonymisation, concerning identifiable data into non-identifiable data. Following this case, there was a guidance note on the concept of "personal data" for the *Data Protection Act 1998* in UK. It states that:

> "In anonymising personal data the data controller will be processing such data and, in respect of such processing, will still need to comply with the provisions of the Act."

If we apply this rule here, then as long as we recognise the raw biometric image is personal data, the process of extracting the template and storing it separately from other sources, can be regarded as "the process of anonymisation"(if this can be called "anonymous" as Grijpink claims). This process is still covered in the personal data protection constraint. Nevertheless, we have to agree, that this kind of application mentioned by Grijpink is somewhat privacy enhancing, and it managed to make the biometric information not so ditrectly

identifiable. But whether it amounts to the anonymous level that can be excluded from the data protection constraint is still controversial.

3. Storage of biometric data

The storage of the biometric data is perhaps at the centre of concern for biometric technology. There are basically 4 major locations for storing template: in a token or smart card, in a central database on a server, on a workstation or directly on the sensing device. The last two ways of storing biometric information is not as popular as the user cannot authenticate from multiple locations. Hence we will just focus on the first two ways of storage.

The fact that the biometric template is stored in a central database poses several risks about privacy and security (Tuyls, P. and Goseling, J.2004). It is generally accepted that the risk of the reuse of biometric information for an "incompatible purpose" and the possibility of protecting the biometric data against accidental or unlawful access, disclosure, alteration would be relatively lower, when the information is not centrally stored. While central storage is used, encryption is often suggested. Then where would the encryption keys be stored and who would have access to them?

If the key is to be stored by a third party for the purpose of backup, more legal parties such as the certificate authority, and other trusted third parties will be involved. Under a key escrow system, a copy of the relevant key would be provided either directly to a law enforcement agency or to a so-called "trusted third party" that could be required to release the key to government agencies under certain circumstances. It may significantly diminish the attractiveness of encryption to users. Obviously, any involvement by a third party increases its vulnerability. Personal information including biometrics will be collected and handled during the process, and there may be security and privacy concerns. (Greenleaf, G and Clarke, R.2005)Moreover, a key escrow system would also impose also significant costs on the use of encryption, especially when such systems are to be used on a global scale.

Storing the biometric information on a portable token such as a smart card is often welcomed by data protection advocate, though some security concerns still exists (Svigal, J.1994). The biometric data is not centrally stored, does not traverse the network, and the user will be able to hold their own information. But a legal question arises concerning the ownership of the personal data on the card. It has been argued the data subject only has the right to use the card, but the ownership of the card still belongs to the data controller. This means the data controller may have the exclusive legal right to the ownership of the card and the personal data on the card. This indicates potential risks of abusing this property. According to the legal doctrine, to appropriate a person's name or likeness is a way of invading his or her privacy. (Restatement (second) Torts, §§652 B, C, D) Privacy therefore has something to do with controlling one's identity. If biometric information is something that makes the individuals special and perhaps unique, it arguably ought to belong to the individual from whom it was ultimately derived. If biometric information belongs to an individual source, it might indicate an exclusive and inalienable right over it. Others may acquire the usage of such information under certain lawful circumstances or through illegal appropriation. Theoretically, under no circumstances should we claim that the individual source loses the right to have legal control over his/her biometric information, which is inherently linked to him. (Rothstein, M.A.1997, ed.)

A problem with smart cards is that people often do not know what is actually stored on smart cards and therefore how to access what is there, nor do they know who is going to get the information on the smart card. A key question is: who controls the back office and is accountable for the subsequent use, disclosure accuracy and security of the biometric data gathered and distributed via a smart card? In cases when biometric verification is used widely for multi-application, it is necessary to address the rights and responsibilities of the card issuers, the data controllers and the cardholders. Under the data protection principles of Convention 108, EU data protection directives, and the guiding principle of smart cards, these issues have not been clearly addressed. (Neuwirt, K 2006)

4. Compulsory and voluntary

There is evidence to suggest that people are willing to accept some loss of privacy in exchange for enhanced security. The problem with the use of biometric technology is whether the choice is left to the data subject or made for them.

In the European context, it is generally suggested that in the public law domain, where compulsory collection is adopted, the data subject should be informed, and be aware of the purpose of the collection and the identity of the controller (Consultative Committee 2005). The personal data should be obtained and processed fairly and lawfully in accordance with article 5 of Directive 95/46/EC. While in the Private law domain, "it is often 'assumed' that the data subject has a free choice." (Consultative Committee 2005). It is vital to notice that the consultative committee uses the word "assume", which indicates it is also possible or legal for the private

sectors to adopt the use of biometric technology without "free choice". Simultaneously, the committee also pointed out that

> Committee notices that similar systems started in the past with a free choice for the client but evolved through a mass application and the acceptance of nonnegotiable standard contracts or clauses into a situation where de facto there is no longer a choice for data subjects that want to take part in ordinary life. Although there is no law obliging citizens, technology has become so pervasive that for individuals that want to take part in daily life a real choice is no longer available. (Consultative Committee 2005).

However the committee stopped short, without giving more suggestions and comments on this situation. Is there a bottom line for this? What kind of attitude would the committee like to have? Are there any recommendations? It became very difficult to detect the real intention of the committee. In Paul de Hert's report (2005) , it was clearly suggested that "consumer law should make clear that anyone who is asked to voluntarily submit biometric identifier be fully informed, competent to understand the impact of actions and under no threat of harm to agree to such action, which means possible alternatives are provided without too much inconvenience." It is significant to emphasize that "consent" should be free and informed, but Paul de Hert 's report is still silent on whether it is legal to adopt compulsory biometric data collection in the private domain.

In the US context, a clear answer has been given in the case law decisions. In 2002, the Maryland Court of Special Appeals in *Messing v. Bank of America* (143 Md. App.1792 A.2d 312(2002)) became the first court to decide the issue of mandatory collection of biometric identification in the context of commercial transactions. In this case a non-bank customer was required to provide a thumbprint before a check. The bank was sued by this customer for this request. However, the court decided that "the Bank's request of a thumbprint upon the instrument constitutes a request for "reasonable identification" within the meaning of Md. Code, Commercial Law Article, §3-502(b)(2)(ii)." (143 Md. App.1792 A.2d 312(2002)) Following this case, there were also many similar cases that involve mandatory commercial use of biometric data decided by the superior courts of other states. As far as the author knows, since there is not yet a case brought to the federal court, it is clear that it is generally held that the collection of biometric data in the private sectors is reasonable in terms of scope and necessity. However there are also dissenting views. For example, in the case *Messing v the Bank of America*, it was commented:

> Today, honest citizens attempting to cope in this world are constantly being required to show or give drivers' license, photo identification cards, social security numbers, the last four digits of social security numbers, mothers' "maiden names,"16 digit account numbers etc. Now the majority takes the position that it is "reasonable" for banks and other establishments to require, in addition, thumbprints and fingerprints. Enough is enough. The most reasonable thing in this case was petitioner's "irritation with the Bank of America's Thumbprint Signature program." (143 Md. App.1792 A.2d 312(2002))

The mandatory use of biometric technology in the private sector needs to be grounded with a strong legal basis. It is very difficult to decide to what extent the authentication is secure enough. But what deserves attention is that the use of biometric information is in itself a trade off of the data subjects' privacy and security against the private entities' security and data subjects' convenience. The technology of biometrics is not as mature and accurate as what commercial entities have claimed. From the data subject's perspective, this use of biometric information may bring some convenience and to some extent some sense of security, but there is no guarantee that they will still make the same choice when they really understand the security and privacy risks they are exposed to when using biometrics. From the private entities' side, once they get control of the biometric data of the data subjects, they are in a sense free. The data subjects typically must rely on their honesty in adhering to the security and privacy policy for protecting their personal data. Even if the data subjects have consented (bearing in mind it is also doubtful if this is a "real" consent in the legal sense we mentioned.) to centralized template storage under the program of the private entities' control, the private entities might still violate the scope of consent without notifying the data subject. Unlike in the public sectors where stricter audit from the public and law enforcement sections are available and a relatively stronger legal basis for using biometric technology are accepted, the private sector is not eligible enough to adopt mandatory use of biometric technology. Hence, it may not be appropriate to allow mandatory collection of biometric data from the private sector in general.

5. Necessity of using biometrics in the private context

Sorting out a community's common view of what constitutes necessary or reasonable criteria for using a controversial technology in certain circumstances for identification or verification warrants serious public debate. This seems to be a subjective question that is to a large extent dependent on the judiciary or the data protection

authority's margin of appreciation. However, despite the subjectivity, reasonable decisions can only be made after evaluation of various objective factors. It will be meaningful to find out the various factors the judiciary or authorities use to reach different conclusions on similar questions.

As we noted in the above section in the case *Messing v Bank of America* (143 Md. App.1792 A.2d 312(2002)) , the Court of Appeals of Maryland in the US, found a thumbprint as a "reasonable identification" requirement set forth in federal banking regulations and state commercial transactions law for the following reasons:

1. A thumbprint is specified as one of a number of means of signature and authentication in the Maryland Uniform Commercial Code (UCC) (§1-201(39)).
2. Other biometric identification means have been upheld in other non-criminal circumstances not to be an invasion of privacy, and is reasonable and *necessary* for the growing means to check fraud.
3. The thumbprint is not unreasonably inconvenient and the inkless method used was even less intrusive than traditional fingerprinting which has been repeatedly upheld as an "unobtrusive" form of identification
4. The fact that a thumbprint does not permit immediate identification but only assists in remedial prosecution is irrelevant, since both functions are valid purposes of a "reasonable identification" requirement (143 Md. App.1792 A.2d 312(2002))

The first two reasons were listed in response to the petitioner's argument that the use of biometrics is a violation of privacy. The third reason is also relevant in the sense that it discussed the intrusiveness of the inkless "thumbprint". The fourth reason is in response to the petitioner's arguments that the thumbprint was not actually used for identification at the time it was provided, since the petitioner was not a usual customer of the Bank of America, and the bank actually had no storage of his thumbprint before. Considering the relevance of privacy issues here we will just focus on the first three reasoning from the court.

The legal basis for the first reason states that: " 'Signed' includes any symbol executed or adopted by a party with present intention to authenticate a writing."(Maryland Uniform Commercial Code (UCC) §1-201(39)). The court is correct in agreeing that this broad definition can possibly include any kind of biometric signatures. However it is significant to point out that this provision can only indicate that the UCC accepts a biometric signature as an *adequate* means of providing authentication. There is no more indication that it also amounts to a *necessary* means for authentication in the private context and therefore mandatory collection should be regarded as reasonable. As we mentioned earlier, the problem of using biometrics in a private context is not whether it is strong enough to be used as identification, but whether it is disproportionate to the task at hand when using it.

The legal basis of the second reason is that there have been precedents from other courts which upheld that biometrics can be used as a reasonable identification method. It is true that many other cases have approved the use of biometrics in a number of other non-criminal situations, for instance, *Thom v New York Stock Exchange*, 306 F Supp.1002 (1970), *People v Stuller*, 10 Cal App3d 582 (1970) etc. Nevertheless, all these cases that dealt with biometrics happened in the public domain and the court decisions were based generally on the discussions about whether there were Fourth or Fifth amendments violations in the US constitution. Using these precedents as a ground for a final decision about a private domain case applying different legal resources does not seem to be very persuasive.

The third reasoning is based on the subjective element that the inkless thumbprint is less intrusive than the thumbprint using ink. However, it is critical to note that an image that has become digitally stored in the computer, is actually much easier to be preserved and copied than an image on paper. Consequently, the inkless thumbprint has more risks of misuse than an image on paper.

In Europe, under the EU Data Protection Directive, the data protection authorities tend to be more cautious in deciding the level of "necessity" in adopting biometric technology. In November 2005 the Swedish Data Protection Authority upheld the case of prohibiting the adoption of fingerprint as an identification means in a school for pupils entering the school canteen for food. (Datatinspektionen 2005)In February 2006, the Norwegian Data Protection Authority (datatilsynet) published its policy of prohibiting the use of biometrics as an identification /verification method at various private contexts, such as at an airport, for employees' entrance to companies, at training centre's wardrobe. (Datatilsynet 2006) The listed reasons are summarised as follows:

1. According to the Norwegian Personal Information Act art-12, the *unique and precise* identification measure is only useful when there is an *actual objective* need for ensuring identification and the method is *necessary* for such identification. Fingerprints, the iris and other kind of biometric identification fall in the scope of or unique identification measure", and therefore the adoption of such measures must fulfil the strict conditions. The data protection authority did not find any of the above cases that fulfil these requirements of law.
2. It is not meaningful to distinguish the raw biometric image and the code stemming from it, provided that this code is identifiable to certain individuals.

3. It is not meaningful to state that encryption is adopted in connection with the use of biometrics and therefore makes it difficult to be misused. These are just measures that need to be adopted for security reasons when the basic objective of using such measure fulfils the law's requirements.

Datatilsynet went on to state that there maybe some revisions of the provision in the Data Protection Act art 2 in the near future, so that biometrics can be used as a *verification* method when it is necessary. The strict data protection provision in Norwegian law is the basis of the data protection authority's decision. Nevertheless, it is not difficult to notice that the Norwegian Data Protection Authority's attitude towards biometric technology is also in accordance with the various reports from the EU. (Hert,P.D. 2005)

1. It recognized biometric technology as a unique identification measure and which needs special attention and it considered the use of biometrics in these circumstances as not necessary as there are other less intrusive alternatives. (I K Lykke Drift AS, 05/0133944/AFL, 16. Feb, 2006)
2. It considers that both biometric image and biometric template are identifiable, and falls into the scope of personal data.
3. It recognized the value of encryption for protecting privacy.
4. It is aware of the difference between "identification" and "verification", and indicates that in the future, biometric verification may be allowed under certain circumstances.

Compare with the American court's reasoning in the case *Messing v Bank of America*, the Norwegian Data Protection Authority's decision sounds more legally reasonable. However "necessity" of using certain identification measures such as biometrics in certain circumstances still remains to be an arguably vague term. Neither of the two decisions clearly clarified the content of "necessary".

The notion of "necessary" generally denotes "that must be had, obtained or done, needed" (Longman Dictionary of Contemporary English, Longman Group UK Limited 1987, p 694). One substantial indication is not having other alternatives, and is inevitable for fulfilling the goal. Accordingly when used to label issues that arise in biometric applications, "necessary" may possibly refer to the following concerns:

1. There is an inevitably strong need for a *permanent* and *unique* "identification" or "verification" method.
2. The benefits of using biometric identification outweigh the risks that it may bring.
3. There are no other alternative verification or identification methods that can fulfil the task in the circumstance.

The first criterion stems from the characteristic that biometric technologies are based on physical or behavioural characteristics that are unique and permanent for identifying individuals. The fear is that such a unique number would facilitate searches in any database in which it resided. Suppose that the use of biometric information is not strictly restricted, or evaluated for its necessity, the various environments where one might provide biometric information in the public and private sector: banking, medical, public service, retail, training clubs, employment and other sectors. The prospect of information linkage and collection is extremely problematic.

This leads us to the second criterion- the balancing of benefits and risks. It has been pointed out by many that the use of biometrics is directly associated with various privacy and security related concerns, (Clarke, R.2001and Rosenzweig, P.etc.2004) such that it is impossible to discuss biometrics without addressing the negative perceptions which surround its usage. Some of the fears include that it will be gathered without permission and used for a multitude of purposes other than the one for which it was initially consented, will be used for tracking the people for surveillance and social control, will also destroy anonymity, cause permanent identity theft, and raise cultural and religious concerns. In the light of these and other concerns, the adoption of this technology needs serious evaluation.

Passwords and tokens are traditional verification methods, to identify people. In spite of the shortcomings of these verification methods, they may be easily shared, stolen or lost. These methods may be used appropriately and the security level of these methods is actually no worse than biometrics. One very interesting keyspace (Rosenzweig, P.etc.2004) comparison of password versus tokens and biometrics regarding their security has been published by Lawrence O' Gorman, as follows:

Token>= password >Iris>Fingerprint, PIN> Voice >face (Rosenzweig, P.etc.2004)

From this we can see that apart from the human factors, biometrics is in fact no more secure than the traditional verification factors, such as a well chosen password, and a well protected token. Its advantage lies in the fact that it is so closely linked to the human user, and it is convenient to some extent, and avoids the possible troubles caused by a human's bad memory, careless, or malicious intention. The use of biometrics has long been

criticized as overkill to the task at hand, and it suggests we reconsider whether it is sufficient to use a password or token to verify the entrance of the training center or should such an invasive technology be adopted?

6. Conclusion

Biometric technology is a new technology with various applications. Concerns about it extend deeply into law and morals. What are the controversial legal problems raised by various biometric applications? And how should they be addressed? The answers I have offered have just canvassed a small section of the whole picture. To some extent, in the biometric domain, it depends on the context (both jurisdictions and applications) of whether our privacy will be protected or to what extend it may be protected.

Although biometric technology promises to some extent a revolution in the level of security and convenience of personal identification and verification, we should also pause to consider some of the risks of its widespread implementation as we embrace this technology. Specific legal measures are called upon in response to these risks. This article has attempted to explore the major privacy interests concerned in various biometric applications. In this regard, various technical elements and application policies are of relevance to the extent privacy may be affected.

To withstand legal and policy challenges, the current initiatives have provided some clue for shaping the legal framework that will govern the biometric technology in the future. However, they are far from adequate in providing an effective remedy for dealing with the various legal problems raised by the new technology. Mindful of the regulatory gap, some recommendations are put forwarded:

1. Based on the fact that various kinds of sensitive information can not be technically excluded from the biometric authentication process, biometric template and biometric image in general should be regarded as sensitive personal data in the legal sense.
2. As a technology born to identify people, whether the use of biometric data can be regarded as anonymous, still remains controversial.
3. While the future course of the biometric industry and its influence is not yet clear, the wide spread use of the technology should be strictly controlled. In the private domain, compulsory collection of biometric data should be prohibited, and meaningful alternatives should be provided.
4. When evaluating the necessity of using biometric technology, with the strong need for the unique and permanent verification/identification there should be a check and balance of the benefits and risks, and the existence of possible alternatives should all be taken into account.

Reference

1) Ashbourn, J. (2004) Practical Biometrics: from Aspiration to Implementation, Springer professional computing, London: Springer.
2) Bing, J (1972) Classification of personal information with respect to the sensitivity aspect, Proceedings of the First International Oslo Symposium on Data Banks and Society
3) Blas,D.A.(2005) Privacy, the Use of Databases in Forensic Disciplines: a Balance of Interests, in J.F. Nijboer & WJJM Sprangers (eds.); OC,(499-5111), 501-503
4) Bromba, M. (2003) On the Reconstruction of Biometric Raw Data from Template Data. At http://www.bromba.com/knowhow/temppriv.htm , last accessed Jan 2006
5) Bygarve, A.L. (2003) the body as Data? Reflections on the Relationship of Data Privacy", Body as Data Conference, Melbourne, Australia September 8, 2003. At http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/CF51D885BA101AACCA256E050012CBA5/$FILE/Bygrave%20paper.pdf#search=%22%22body%20as%20data%22%22 , last accessed Sep. 2006
6) Clarke, R. (2001) Biometrics and Privacy, at http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html, visited May, 2005
7) Commission (1992), the Commission's Commentary with Respect to its Amended Proposal for a Data Protection Directive of 15.10.1992(COM (92)422final-SYN287), p.9. See also its commentary with respect to the original Directive proposal of 24.9.1990(COM (90)314final-SYN287) p15.
8) Consultative Committee of the Convention for the Protections of Individuals with Regard to Automatic Processing of Biometric data (2005), Progress Report on the Application of the Principle of Convention 108 to the Collection and Processing of Biometric data, Feb. http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/ , last accessed Jan 2006
9) Cullagh, K. M (2007) Data sensitivity: resolving the conundrum, 2007 Annual conference Hertfordshire 16-17 April

10) Cytowix, R.E. (1996) All in the Genes, Washington Post Sep1 1996; N. Hawkes, Fingerprint Clues to Health, Times of London, Feb 26,
11) Darren, D.W, and Silver, B.D.2004. Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America. American Journal of Political Science, 48(1):28-46
12) Datatinspektionen 2005, http://www.datainspektionen.se/nyhetsarkiv/nyheter/2005/november/2005-11-22.shml , last accessed Nov, 2005
13) Datatilsynet (2004) PVN-2005-12:Klage på Vedtak om Begrensninger i Adgangen til Kameraovervåking av Bussenes Publikumsområder. at http://www.personvernnemnda.no/vedtak/2005_12.htm, last accessed Sep. 2006
14) Datatilsynet 2006, http://www.datatilsynet.no/templates/Page____1342.aspx, last accessed Feb. 2006
15) Data Protection Working Party (2003), Working Documents on Biometrics, Aug1. At, www.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp112_en.pdf, last accessed Jan 2006
16) Grijpink, J. (2001) "Privacy Law: Biometric and Privacy", Computer Law and Security Report, 17, No. 3, pp154-160.
17) Greenleaf, G and Clarke, R.(2005) "Privacy Implications of Digital Signature", at http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html , last accessed Aug. 2005
18) Hert, P.D.(2005) Biometrics: Legal Issues and Implications, European Communities. At http://www.statewatch.org/news/2005/apr/jrc-biometrics-paul-de-hert.pdf , last accessed Jan 2006
19) Johnson,M.L.(2004) The Biometrics and the Threat to Civil Liberties, Computer, vol. 37, no. 4, pp. 92, 90-91, Stanford University, April
20) Hancock, E. and Hendricks, M.(1996) In Short- Health and Medicine, John Hopkins Magazine, June.
21) ICO (2006) Annual Track Survey, retrieved June 20, 2007 from http://foia.blogspot.com/tracindivs2006.pdf
22) Miller, B. (1988), "Everything You Need to Know about Biometric Identification", Personal identification News 1988 Biometric Industry Directory, Warfel & Miller, Inc., Washington DC, January.
23) Neuwirt, K (2006) Council of Europe Report on the Protection of Personal Data with Regard to the Use of Smart Cards prepared by the at http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/Reports/T-SmartCards%202001.asp , last accessed Feb. 2006
24) Nicoll, J.E.J. Prins, M.J.M. (2003), Digital Anonymity and the Law: Tensions and Dimensions / ed. by C. Nicoll, J.E.J. Prins, M.J.M van Dellen. The Hague: Asser Press.
25) Phred, D. (2004), "Testing the TV Tuners and Fingerprint Checks in Cell Phones in Japan". Wall Street Journal, June 3
26) Prins,C. (1998), Biometric Technology Law, Making Our Body Identify for Us: Legal Implications of Biometric Technologies, Computer Law & Security Report Vol.14 no.3.
27) Rinehart,G.(2006), Biometric Payment: the New Age of Currency, http://www.hotel-online.com/News/PressReleases2000_1st/Mar00_BiometricCurrency.html , last accessed Jan 2006
28) Rosenzweig,P.etc.(2004) Biometric Technologies: Security, Legal, and Policy Implications. Legal Memorandum, the Heritage Foundation, No.12 June.
29) Rothstein, M.A. (1997) ed. Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic era, Yale University Press, New haven and London.
30) Soutar, C (2002), Biometric System Security, in: Secure No. 5, p 46-49.
31) Svigal,J.(1994), Smart Cards-a Security Assessment, Computer and Security, 13 pp107-114
32) Tuyls,P and Goseling, J.(2004), Capacity and Examples of Template Protecting Biometric Authentication Systems. D. Maltoni and AK Jain (Eds): BioAW, LNCS3087, pp158-170.
33) Wacks, R (1989) Personal Information: Privacy and the Law, Oxford: Clarendon Press
34) Wayman, J. L. (2000), a Definition of "Biometrics", National Biometric Test Center Collected Works, San Jose State University.
35) Wong, R (2007) Data protection online, alternative approaches to sensitive data? Journal of International Commercial Law and Technology, Vol2, No1