Saying NO To Biometrics

By Guru Dev Teeluckdharry (MBA – University of Leicester)

'Technological progress has merely provided us with more efficient means for going backwards.' - Aldous Huxley

Introduction

The society today is being revolutionised with Biometrics, which is a term derived from the words *'bio'* (meaning life) and *'metrics'* (meaning to measure).

Biometric technologies include fingerprint recognition, face recognition, hand geometry, iris scanning, voice recognition, signature recognition, retina scanning, ear/lip motion recognition, body odor analysis, skin reflection analysis, nail bed analysis, body shape analysis, dental analysis, and DNA recognition. (Langenderfe and Linnhoff as cited in Roberts and Patel).

The field of biometrics is evolving at a very fast pace. Passwords, usernames and codes are things of the past. Nowadays, governments are opting for biometric technologies with respect to National ID cards, social security cards, e-passports and driving licenses. Furthermore, these technologies are also being put forward as arguments worldwide, to help resolve problems such as international terrorism, crime prevention, civil war, drug trafficking, identity theft, computer and internet crime, border control, illegal immigration, financial scam, fraud, security and unlawful activities in the society. But how far are they effective? Are we conscious that such technologies are fraught with risks and dangers?

Courts and Biometric Data Schemes

Courts' decisions with respect to a good number of biometric data schemes have pronounced that the collection, processing, handling and storage of biometric data in the society are interferences with the right to privacy, integrity and confidentiality. To this point, such interferences may exceptionally be justified if there are adequate legal safeguards against hacking, abuse and misuse of data, and exclusively

because "the right to privacy is a basic constitutional right which however, just like all other fundamental rights, is not absolute." (Oxford Pro Bono Publico).

In *S and Marper v United Kingdom* (2008), with respect to *'collection of fingerprints, cellular samples and DNA samples'* by the police in the UK from the applicants, it was held by the Grand Chamber of the ECtHR (European Court of Human Rights) that the retention and storage of such *'personal data'* was an interference with the right to privacy as per Article 8(1) of European Convention on Human Rights (ECHR). Though accepting that it may be absolutely legal to collect DNA and fingerprints of suspects in detection and prevention of a crime, the ECtHR (European Court of Human Rights) in this case also emphasized that there should be appropriate [legal] safeguards to prevent the misuse of personal data and same cannot be stored indefinitely. (Oxford Pro Bono Publico).

In *Whalen v Roe* (U.S Supreme Court) (1977*),* the Supreme Court did highlight uncertainties about privacy and emerging technologies, and Mr. Justice Stevens expressed the remarks: *'We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other government's files'*. Similarly, Mr. Justice Brennan also indicated: *'The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology'*. (Oxford Pro Bono Publico).

In 2012, the French Constitutional Court (the *Conseil Constitutionnel*) regarding the legislation for a national Identity biometric card containing information such as face and fingerprint recognitions, and provision for the creation of a national database stated that the Act's aim is to prevent identity fraud. However, the *Conseil* observed that the legislation surpassed this legitimate purpose because it authorized the police and other law enforcement agencies to have access to the database for other purposes unrelated to the prevention of identity fraud. Therefore in such circumstances, "the *Conseil* found that this was a disproportionate restriction of the right to privacy. It should be noted, however, that the *Conseil* did not take issue with the creation of a population-wide biometric database per se." (Oxford Pro Bono Publico).

In *Nahon v Knesset* (2012), the condition of collecting biometric data in a centralized database was debated in the Israeli High Court of Justice. "In the wake of the 2006 theft and dissemination of Israel's Population Registry, containing data on 9,000,000 Israeli citizens, the Justices were particularly concerned that a centralized biometric database would bring greater security risks." (Oxford Pro Bono Publico).

In 2014, The Supreme Court ordered that the Aadhaar [biometric National ID] card in India will not be mandatory for availing any service. In the same context, the court has also "directed the Unique Identification Authority of India (UIDAI) not to share any information pertaining to an Aadhaar card holder with any government agency without the prior permission of the card holder…" (IBNLive).

Instances of Miscarriages of Justice based on fingerprints evidence

In 1997, Shirley McKie was arrested by The Scottish Police Services Authority. This case proved that fingerprinting as biometric data recognition in solving crimes was prone to human errors. Ms McKie was accused of perjury after she stated that a fingerprint found at the home of murder victim Marion Ross, was not hers. She always denied entering the property, but four fingerprint experts maintained that the print belonged to her. Later on, when the truth revealed that the fingerprint was not hers, she was cleared and awarded £750,000 in compensation. (BBC NEWS).

In 2004, Brandon Mayfield (a lawyer of civil and immigration lawyer, practicing in Portland, Oregon) was arrested wrongly with respect to an investigation of the terrorist bombing attack in Madrid, Spain. The FBI averred that his fingerprint was found on a bag containing detonation devices in Spain. The government then announced that the FBI had committed a *'multitude of errors'* in its identification of Brandon Mayfield, and as a result this case was dismissed. He was offered $2,000,000 as compensation. (Champion Magazine).

Legitimate Reasons to Say NO

First, fingerprint recognition has criminal connotations and as such it could be perceived as abusive by minority groups whose dignity could be hurt. (Mordini and Petrini, 2007).

Second, fingerprint recognition is also associated with illiteracy, and people who do not know how to sign their names are often asked to use their thumb fingerprint in lieu of a written signature. Many people could feel embarrassed in a modern culture.

Third, "biometrics has proved inaccurate and ineffective in fighting identity fraud. In 2011, a French report revealed that 10% of biometric passports were fraudulently obtained for illegal immigrants or people looking for a new identity". [LeParisien, *'Plus de 10 % des passeports biométriques seraient des faux', L'infalsifiable a un maillon faible!*...]. (ELECTRONIC FRONTIER FOUNDATION).

Fourth, "biometric systems are never 100% accurate as they are statistical." (TECHNICAL REPORT SERIES). Both human and computer errors are inevitable. Such scenarios have already taken place in the cases of Brandon Mayfield and Shirley McKie (who were arrested unjustly and) where there were *'human errors'* that resulted in instances of miscarriages of justice based on fingerprints evidence.

Fifth, the biometric database in itself is a tool that symbolizes tyranny and persecution, from the historical perspective. "In their referral to the *Conseil*, French parliamentarians quoted Martin Niemöller's chilling poem *'First they came. '* They argued that had this kind of database existed during WWII, the Nazis and collaborators in Vichy France could have more easily arrested French Résistance fighters based on their fingerprints or facial scans." (ELECTRONIC FRONTIER FOUNDATION).

Sixth, databases storing biometric data could be hacked, stolen and exposed publicly on the web alike the case of the theft of the biometric database of Israel in 2006 containing information of 9,000,000 Israelis (living and dead). (FastCompany). This could expose a whole nation to an unexpected catastrophe. Radical terrorists are always on the threshold to grab such opportunities to perform hostage-taking, ethnic cleansing, terrorist attacks, anti-Semitic crimes and mass murder. It is to be emphasized that

the security of databases on servers and networks have also been called into question, since the hacking of U.S data brokers networks containing social security numbers, birth records, and credit and background reports of many prominent Americans, including First Lady Michelle Obama, Bill Gates, Beyonce Knowles, Jay-Z, and Ashton Kutcher took place. (INTERNATIONAL BUSINESS TIMES).

Seventh, minority people could be stigmatized. Based on the FRVT of 2002, Givens concluded that *'Asians are easier (to recognize) than whites, African-Americans are easier than whites, other race members are easier than whites, old people are easier than young people, other skin people are easier to recognize than clear skin people…'*. As a result, biases could prevail and this would be unethical for a whole community. Disabled citizens lacking physicals characteristics using a biometric facility could suffer discrimination. (Chinchilla, 2012). Social exclusion and inequalities could also be the by-product where underprivileged people could suffer.

Eighth, the "idea of security is non-existent in today's technology and the integration of biometric technology would only give the *'illusion of security for the short term'*." (Roberts and Patel). A very vivid example demonstrating this analysis, is the "hacking of Apple's TouchID by the biometrics hacking team of the Chaos Computer Club (CCC) which used a fingerprint of the phone user, photographed from a glass surface to create a fake finger that could unlock an iPhone 5s secured with TouchID." (Activist Post). This proves that the sacrifice of our biological information on the basis of a false feeling of security and privacy for convenience, is not creditable.

Ninth, there is the imminent risk of Function creep (where original data could be used for secondary purposes). (Kindt, 2007).

Tenth, Spoofing (*[where] 'an artificial finger made of commercially available silicon or gelatin, can deceive a fingerprint biometric sensor'* ((Matsumoto, 2002) as cited in Dimiriadis, 2004)) of "biometric systems for misappropriation of biometric data is a realistic security threat". (Kindt, 2007).

Eleventh, Mimicry Attack could take place where pictures and speech synthesis tools could deceive face and voice recognition systems. (Dimiriadis, 2004).

Twelfth, mandatory biometric National ID cards could lead to abuse by the police which as a matter of routine could request the presentation of such a card from anybody (especially motorists) in unlawful circumstances at any time. This reminds us of the cases of *Willcock v. Muckle* in 1951 and *Brown v. Texas* in 1979.

Thirteenth, biometric data is *'sensitive personal data'*. "The special characteristics of biometric data are: (1) they are health and genetic related, (2) they can be used as relative unique and universal *'key data'* for getting all kinds of personal information (such as race) ". (Hu, 2008).

Last but not the least, biometrics could be exploited for unlawful surveillance resulting in severe erosion of civil liberties, interferences with right to privacy and violation of human rights. It is a reality that, the *'Surveillance Society'* which is already massive and (especially since 9/11)), is growing much faster than other industries (Wood and Ball, 2006). At this point in time, we are refraining from using the term *'Big Brother'* which might be linked with conspiracy theories where there would be no legal evidence to substantiate its existence. Rather, we are using the term *'Surveillance Society'* which is technical and accurate. Powerful CCTVs with facial recognition are already being used for tracking purposes in the *'Surveillance Society'*. (Wood and Ball, 2006). The RFID technology would just be a catalyst in accelerating tracking. In U.S, all passports are now tagged with RFID chips and several states now do issue RFID *'enhanced driver's licenses'* including Michigan, New York, Vermont and Washington. (Hu, 2013). "In Shenzhen, Southern China they are implementing RFID readers to track the movements of citizens [in a sophisticated manner]: *'all citizens have an ID card with a chip so that they can identify who is in what part of the city at any point in time'*. (MICHAEL Journal) ". It is to be emphasised that the chip in the National ID card has not only a number, but also a "person's work history, education, religion, ethnicity, police record, [medical record], and reproductive history. Wal-Mart, Best Buy, the U.S Military and many other agencies around the world, are already implementing the use of RFID chips. In London, police authorities announced that they were putting RFID chips on the entire police force." (MICHAEL Journal). In addition to such possibilities, merging of digitalised biometric National IDs (including a *'cardless'* ID system) and Social Security cards with GPS-RFID tracking technology, could be carried out to "facilitate exponentially

the convergence of *'cybersurveillance-24/7 body tracking'* [that is creation of a virtual security checkpoint by recording movements of people at the time of credit card swipe or smartphone read requiring biometric National IDs at certain points of entry or exit] and *'dataveillance-360° biographical tracking'* [that is the use of information linked to the data captured through the issuance and operation of such a digitalized biometric National ID system, to assess characteristics and patterns of those who possess and use such cards, smartphones, or other digitalized IDs. This could be done indiscriminately, such as through the *'mass cybersurveillance'* of ordinary citizens. This data could be used to target individuals or classifications of individuals—such as targeting groups based on immigration status, national origin, credit history, or zipcode—for additional scrutiny or investigation] ". (Hu, 2013).

Biometrics in the Mauritian Context

In Mauritius - do we have a human rights culture? Are we conscious about the implications of the biometric National ID card and database (MNIS – Mauritius National Identity Scheme) with regard to our basic fundamental rights? Are we going to learn from our own mistakes or should we learn from the mistakes of others?

Should we take note of the U.K, where the biometric National ID card was introduced by the ID Card Act 2006 and then four years later in 2010 the Identity Document Act was passed in order to scrap its biometric National ID card scheme alongside with its biometric passports, dismantle its biometric ID database and physically destroy the hardware of its centralized register (ELECTRONIC FRONTIER FOUNDATION and the guardian)?

Should we all (including the Members of the Mauritian Parliament) give a standing ovation to Mrs Theresa May (The former Secretary of State for the Home Department, U.K) who while introducing the first piece of legislation regarding the "Identity Documents Bill on 9th June 2010 said the following before the parliament**:** *'The national ID card scheme represents the worst of government. It is intrusive and bullying, ineffective and expensive. It is an assault on individual liberty which does not promise a*

greater good. The Bill is, therefore, partly symbolic. It sends a message that the Government are going to do business in a different way. We are the servants of the people, not their masters, and every action that we take must be considered in that context...We have no hesitation in making the national ID card scheme an unfortunate footnote in history. There it should remain-a reminder of a less happy time when the Government allowed hubris to trump civil liberties...In bringing forward this stand-alone Bill, we are now seeking swift approval to enable us to abolish both the ID cards and the National ID register ([which] contains the biographic and biometric fingerprint data of cardholders)...Moreover, ID cards would not make us safer or beat benefit fraud. Benefit fraud usually involves people lying about their personal circumstances rather than their identity. Turkish and Spanish ID cards stopped neither the Istanbul bombers in 2003 nor the Madrid bombers in 2004; nor did German ID cards prevent terrorists plotting 9/11 in Hamburg. As Charles Clarke, the former Home Secretary, said after the 7/7 attacks here in London' (Parliament of U.K)"?

It is to be noted that one late Dr. Rajah Madhewoo did challenge the MNIS Scheme before the Supreme Court of Mauritius in 2015. Unfortunately, the court rejected his petition and it upheld the validity of the card. However, it stressed that the indefinite retention of biometric data and fingerprints of Mauritians constituted an obstacle to the Constitution. According to Dr. Rajah Madhewoo, this judgement of the Supreme Court was 'contradictory'. He then sought the intervention of the Judicial Committee of the Privy Council of the UK to pronounce on the matter. According to Mr. Sanjeev Teeluckdharry (the legal counsel representing the late Dr. Rajah Madhewoo) the biometric identity card infringed the right to liberty as guaranteed by the Constitution of Mauritius. That's what he told the Law Lords. The lawyer explained that any person empowered by this law could force a citizen to produce his identity card and any refusal would result in a maximum prison sentence of five years as well as a fine not exceeding Rs 100,000. "We would become a surveillance State rather than a democratic state", declared Mr. Sanjeev Teeluckdharry. But the Law Lords had asked the Mauritian lawyer not to speculate on the potential dangers of the biometric ID card. "If the government starts this, then you can have an argument. But the law does not allow this. You have to show that the risk is a real one," pointed out the Law Lords. But Mr. Sanjeev Teeluckdharry insisted that the

biometric identity card could be used "for perverse purposes and in violation of the Constitution of Mauritius". He said in particular that the card could be used to track individuals and even contain data relating to the cardholder's state of health. The Law Lords had once again drawn the attention of Mr. Sanjeev Teeluckdharry to his "tendency to speculate on the potential dangers" of the biometric ID card: "You cannot assume the worse and we must not assume the worse. All this is speculation. If it happens you may raise the point. You can challenge it when it happens," said the Law Lords. As for Mr. Sanjeev Teeluckdharry, he argued that we must think of the worst: "My Lords, we have to assume the worse".

In its judgement on 31st October 2016, the Judicial Committee of the Privy Council of the UK (see Michaelmas Term, [2016] UKPC 30, Privy Council Appeal No 0006 of 2016, Jugdement: Madhewoo (appellant) v The State of Mauritius and another (Respondents) (Mauritius) maintained that the points raised on appeal did not affect the assessment of the Supreme Court in any way. The judgement first mentioned the fact that the need to provide fingerprints to obtain a national identity card did not constitute interference linked to criminality, since this obligation applied to the all Mauritian citizens who had reached adulthood. The judgement also took note of the fact that a police officer could have been entitled to ask an individual to produce his identity document and that this representative of the order could also have had access to the minutiae of the fingerprints in the part of a criminal investigation, if it was equipped with appropriate card readers. However, this aspect of things in no way compromised the presumption of innocence enjoyed by the individual in question. This Judicial Committee of the Privy Council of the UK judgement also emphasized that the primary purpose of collecting fingerprints was to ensure that identity cards were issued to the appropriate people. These biometric data were stored in a register during the preparation of the identity card, and they were destroyed upon delivery of this card, following the judgement of the Supreme Court dated 29th May 2015.

Late Dr. Rajah Madhewoo then appealed against the decision of the Judicial Committee of the Privy Council of the UK on 15th December 2017 at the The United Nations Human Rights Committee (HRC) to seek redress against the MNIS Scheme of Mauritius. In a decision dated 21st July 2021, the HRC considered that late Dr. Rajah Madhewoo had been indeed accurate and sincere in putting forward a complaint under the convention. It found that, in the particular circumstances of the case, storage and retention of late Dr. Rajah

Madhewoo's fingerprint data on an identity card would constitute an arbitrary interference with his right to privacy (Page 8 of the HRC decision, paragraph 7.6.) The HRC also stated that the State of Mauritius "has not responded to Dr. Rajah Madhewoo's claim that retention of fingerprint data on identity cards exacerbates the security lacunae identified by the Supreme Court". The HRC further emphasized that, in these circumstances, it could not conclude that there were adequate assurances and guarantees against the risk of abuse. This was in breach of Article 17 of the convention, which dealt with the right to privacy. Most importantly, the HRC also elaborated that the State of Mauritius was under a strict and genuine obligation to provide Dr. Rajah Madhewoo with an "effective remedy" to the current breach of the convention. "The HRC finally requested the State of Mauritius to review the grounds for the storage of fingerprint data on identity cards. Additionally, Mauritius was under the legal and genuine obligation to take measures to avoid similar serious violations in the future." (Page 8 of the HRC decision, paragraph 9.) The State of Mauritius now has 180 days to report to the HRC on the issues raised in the decision.

Conclusion

Even if the so called judgemental interferences of biometric technologies especially biometric IDs and databases with the human life (in the presence of adequate legal safeguards) could exceptionally be justified legally, there are ethical and social ramifications which illustrate that this is also an intrusion on human rights and should not be permissible at all.

References

[Aubert, 2011] Hérvé Aubert, *'Technologie RFID pour implants dans le corps humain'*, Comptes rendus à l'Académie des CSciences , Special issue on nanosciences/nanotechnologies, March 1st 2011

[Bromba, 2006] Manfred U.A. Bromba, *'The Biometric Society - Risks and Opportunities'*, 2006-11-10

[Brown, 1979] Brown v. Texas, 443 U.S. 47 (1979)

[Butler, 2004] John M. Butler, *'Forensic DNA Typing and Prospects for Biometrics'*, DNA and Biometrics (Mitretek Seminar), May 12, 2004

[Capoor, 2006] Capoor, Sapna, *'Biometrics as a Convenience'*, Security: For Buyers of Products, Systems & Services, Dec2006, Vol. 43 Issue 12, p48-50, 2p.

[Chinchilla, 2012] Rigoberto Chinchilla (2012), *'Ethical And Social Consequences of Biometric Technologies in the US'*

[CHO, 2005] CHO, SUNG-BAE;HONG,JIN-HYUK;YUN,EUN-KYUNG, *'A REVIEW OF PERFORMANCE EVALUATION FOR BIOMETRICS SYSTEMS'*, International Journal of Image & Graphics, Jul 2005, Vol. 5 Issue 3, p501-536, 36p

[COVACIO, 2003] COVACIO, S. (2003), *'Technological Problems Associated with Subcutaneous Microchips for Human Identification'*, (SMHId). In- forming Science.

[Cytowix, 1996] Cytowix, R.E. (1996), *'All in the Genes'*, Washington Post Sep1 1996; N. Hawkes, *'Fingerprint Clues to Health'*, Times of London, Feb 26,

[Dimitriadis, 2004] Christos K. Dimitriadis, *'Biometrics - Risks and Controls'*, INFORMATION SYSTEMS CONTROL JOURNAL, VOLUME 4, 2004

[Hashiyada] Masaki Hashiyada, *'DNA Biometrics'*

[Hu, 2013] MARGARET HU, *'Biometric ID Cybersurveillance'*, INDIANA LAW JOURNAL, Vol. 88:1475, 2013

[Itakura] Yukio Itakura; Toshio Nagashima; Shigeo Tsuji, *'BIOMETRIC PERSONAL AUTHENTICATION SYSTEM USUNG DNA DATA'*

[Kindt, 2007] Els Kindt, *'Biometric applications and the data protection legislation'*, Datenschutz und Datensicherheit 31 (2007) 3

[LIBE] TECHNICAL REPORT SERIES, *'Biometrics at the Frontiers: Assessing the Impact on Society'*, For the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE)

[Lin, 2008] Yue Lin, *'Identifying Legal Concerns in the Biometric Context'*, Journal of International Commercial Law and Technology, Vol. 3, Issue 1 (2008)

[Linnhoff, 2005] Langenderfer, Jeff; Linnhoff, Stefan. ,*'The Emergence of Biometrics and Its Effect on Consumers.'*, Journal of Consumer Affairs, Winter2005, Vol. 39 Issue 2, p314-338, 25p.

[Maestre] Sandra Maestre and Sean Nichols, *'DNA Biometrics'*, ISM 4320-001

[Matsumoto, 2002] Matsumoto,T;H. Matsumoto;K. Yamada;S. Hoshino; *'Impact of artificial fingers on fingerprint systems'*, Proceedings of SPIE, 2002, Volume 4677

[MICHAEL] MICHAEL, *'Global Control through the RFID chip'*, Total Surveillance and a Cashless Society, MICHAEL Journal, Canada

[Mordini, 2007] Emilio Mordini, Carlo Petrini, *'Ethical and social implications of biometric identification technology'*, ANN IST SUPER SANITA, 2007, VOL. 43, NO. 1:5-11

[Olatinwo, 2014] Segun O. Olatinwo; O. Shoewu; Olusegun O. Omitola, *'Iris Recognition Technology: Implementation, Application, and Security Consideration'*, The Pacific Journal of Science and Technology, Volume 14. Number 2, November (2014)

[Oxford, 2013] Oxford Pro Bono Publico, BIOMETRIC IDENTIFICATION AND PRIVACY, *'Comparative research prepared for the Centre for Law and Policy Research, India'*, University of Oxford, February 2013

[Patel] Jarret Roberts and Seja Patel, *'Biometrics: Does Convenience Outweigh Privacy?'*

[Prins, 1998] 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

[Smith, 2008] Charles Smith, *'HUMAN MICROCHIP IMPLANTATION'*, J.Technol. Manag. Innov. 2008, Volume 3, Issue 3

[Waters, 2006] Waters, R, *'US group implants electronic tags in workers'*, Financial Times, 12 February 2006

[Willock, 1952] Willock v. Muckle, [1952] 2 All ER 367

[Wood, 2006] David Murakami Wood and Kristie Ball, *'A Report on the Surveillance Society'*, Public Discussion Document, September 2006

http://edri.org/edrigramnumber10-6french-biometric-database-unconstitutional/

http://www.lemonde.fr/societe/article/2012/03/23/la-nouvelle-carte-d-identite-biometrique-jugee-inconstitutionnelle_1674721_3224.html

http://www.haaretz.com/print-edition/news/population-database-hacked-in-2006-reached-the-internet-1.391812

http://www.bbc.co.uk/news/uk-scotland-glasgow-west-16181875

http://www.nlada.org/Defender/forensics/for_lib/Documents/1107541411.93/

http://news.bbc.co.uk/2/hi/8707355.stm

http://www.fastcompany.com/1790444/dark-side-biometrics-9-million-israelis-hacked-info-hits-web

http://www.activistpost.com/2013/09/a-warning-against-biometric-security.html

http://www.ibtimes.com/michelle-obama-other-public-figures-private-data-hacked-data-broker-giants-1411760

http://www.theguardian.com/politics/2010/may/27/theresa-may-scrapping-id-cards

https://www.eff.org/pages/success-story-dismantling-uk%E2%80%99s-biometric-id-database

http://www.snopes.com/politics/medical/microchip.asp

http://misbiometrics.wikidot.com/dna

http://www.globalresearch.ca/the-implanted-radio-frequency-identification-chip-smart-cards-in-a-surveillance-society/10097

http://www.wired.com/2013/08/student-rfid-chip-flap/

http://news.bbc.co.uk/2/hi/uk/6108496.stm

1: http://www.soundchristian.com/mark/

2: http://www.snopes.com/politics/medical/microchip.asp

http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm100609/debtext/100609-0006.htm#10060953000001

https://www.eff.org/deeplinks/2012/03/french-constitutional-court-bans-law-enforcement-use-biometric-data

https://www.eff.org/deeplinks/2012/06/biometrics-national-id-passports-false-sense-security

http://timesofindia.indiatimes.com/india/Aadhaars-purpose-in-doubt-as-SC-says-its-not-

mandatory/articleshow/22960981.cms

http://ibnlive.in.com/news/withdraw-orders-making-aadhaar-mandatory-for-any-service-sc-to-centre/459875-37-64.html

https://www.eff.org/issues/national-ids

http://eyetrackingupdate.com/2010/11/03/beware-problems-iris-recognition/

http://www.leparisien.fr/faits-divers/plus-de-10-des-passeports-biometriques-seraient-des-faux-19-12-2011-1775325.php

http://www.computerweekly.com/feature/Oyster-Card-The-highs-and-lows-of-Oyster

http://www.thenewamerican.com/tech/computers/item/17688-rfid-implants-the-benefits-vs-the-dangers

Michaelmas Term, [2016] UKPC 30, Privy Council Appeal No 0006 of 2016, Jugdement: Madhewoo

(appellant) v The State of Mauritius

Human Rights Committee, No. 3163/2018, Communication Submitted by Dr. Rajah Madhewoo (represented by counsels Pete Weatherby QC, Erickson Mooneapillay and Sanjeev Teeluckdharry)