



Report of the Second BITE Scientific Meeting

Tuesday 26th April 2005, Rome, Italy.

BIOMETRICS AND PRIVACY

The second scientific BITE meeting was held at the CNR, the Italian National Research Council, in Rome, and was chaired by Professor Ermelando Vinicio Cosmi, director of the CERBIC, the Centre for Clinical Research and Bioethics of the University of Rome "La Sapienza". Partners of the Project, speakers, journalists, members of various Italian academic and public institutions were attending the meeting, for a total of about 25 people.

The program of the day developed, after a welcome delivered by Prof. E.V. Cosmi (CERBIC, Italy), with an introduction to BITE Project by Prof. Emilio Mordini (CSSC, Italy) and three lectures, each followed by discussion and a final wider debate on different aspects that connect biometrics to privacy and ethics.

The issues introduced by the three lectures were the following:

1. **Stefano Rodotà** (former Italian Privacy Commissioner and member of the European Group of Ethics – EGE) spoke about "Body, Privacy and Human dignity"
2. **Kush Wadhwa** (director EMEA of the International Biometric Group) spoke about "Biometrics: a privacy invasive or a privacy sympathetic system"
3. **Mario Savastano** (researcher at Italian National Research Council and convener of the ISO/IEC JCT1 SC37 WG6 on Cross Jurisdictional and Societal Aspects) spoke about "Accessibility in biometrics".

After introducing the BITE Project, Emilio Mordini, explained the specific focus of this second meeting on Biometrics and Privacy. He explicated how privacy issues are no longer only legal issues, and how in late modern societies, these issues are intimately connected with human dignity and the respect of the private sphere. The distinction between private and public comes from moral and political theory: the private realm is that which it is no business of the law. This distinction implies setting boundaries, and in Western societies these boundaries have always passed through the human body. Mordini gave a definition of the body as a "battlefield where private and public realms play their game". Also human dignity, which marks the interaction between private and public spheres, is an embodied concept. "This fact is far more than a simple



claim that the human body must be respected” said Mordini. The definition of dignity is rather a result of the way in which societies conceptualize the body: philosophical and political consequences are immediate. Mordini evoked Michel Foucault: the fact that life, and living being, the species and its reproductive requirements, have moved to the heart of political struggle, is something that is radically new in human history. Foucault gave the definition of “biopolitics” as the form of government taken by a new dynamic of forces that, in conjunction, express completely new power relations. Biopolitics is the strategic coordination of these power relations in order to extract a surplus of power from living beings. Mordini closed his foreword by suggesting that a Foucauldian perspective could add new point of views to the debate on ethical and societal implications of biometrics.

The core issue raised by Stefano Rodotà was the ethics and politics of the “informatization of body”. He started his presentation by posing a question: “What is happening to the human body today?” In his view, nowadays we are facing a deep change in the way in which electronics can be used for changing the true nature of the body. Rodotà’s presentation started from the issue of identification, to move towards the issue of body transformation. According to Rodotà we are entering the trans-human, post human age and we are facing a deep change in human anthropology itself. The body as such is becoming a password, physicality is replacing abstract passwords. Fingerprints, hand and finger geometry, iris, retina, face, voice, signature are increasingly used as a biometric information not only to identify individual, but also to set up permanent categories and for additional control for identification or authentication, verification and confirmation of someone’s identity. The body is growing in its importance once again: it’s becoming a source of new information. Finally the body itself can be technologically altered and primed to be followed and located on a permanent basis. Rodotà gave some examples of the different use of applied digital solutions for health purposes - authorized by the US Food & Drug Administration – and for patient identification – already in use in an Italian hospital. By the way electronic body identification is also used for more trivial purposes: under skin chips have already been in use to replace credit cards and enable quicker and most secure payments in some European discos. Rodotà pointed out that electronic body identification belongs to a wider trend of body alteration, which includes piercing, tattoos, body art. Young people are likely to be more prone to accept body identification via electronic devices because they have already accepted that the body can be manipulated and altered for several other purposes.

Video surveillance, biometrics, implantable microchips, smart cards and RFID technologies are turning us into networked persons. “We are confronted with changes that have to do with the anthropological essence of individuals” stated Rodotà. We are always connected and can be



configured differently so that from time to time we can transmit and receive signals allowing moments, habits and contacts to be traced and defined. For Rodotà this is bound to modify meanings and contents of individual autonomy. Here Rodotà quoted the programme announced on July 19th 2004 by Tony Blair: according to this programme the five thousand most dangerous UK criminals would be tagged and tracked via satellite. Indeed there is a dramatic change in the legal and social status of individuals underlined with this approach: having served a sentence in full will not be enough to regain freedom. The natural body will therefore end up being modified because it will become a post human body that has undergone technological manipulation. Rodotà wonders if these processes can be considered compatible with the human dignity principle which is solemnly affirmed at the outset of the Charter of Fundamental Rights of the European Union. Could identification, authentication or surveillance and transaction security purposes justify whatever use of the human body is made possible by technological innovation? “We shall not lay our arms upon thee” this was the promise made by the Magna Charta in the 13th century: respect for the body in its entirety. This promise is surviving technological evolution, therefore each processing operation concerning biometric data should be considered to relate to the body as a whole, to an individual who must be respected in her/his physical and mental integrity. This is what is expressly provided in article 3 of the Charter of Fundamental Right of the EU. Data protection is one of the most significant components of personal freedom. The use of biometrics can provide new forms of security for all and make everyday activities simpler by increasing identification certainty and making identity theft more difficult. However biometric solutions are not a technological panacea. Public opinion might overestimate their accuracy and associates them with all-round protection against terrorism. This false certainty may lead citizens to progressively become unaware of the risk for their privacy and for the protection of their personal freedom. The issue of democratic legitimacy of security policies is complicated - Rodotà observed – by an increasing “mithridatism”. Society is anaesthetized because the perception of the loss of control over one’s body is cancelled little by little. Democracy goes beyond its being the rule of the political game. It fully incorporates the safeguard of the human dignity: the body and the personal freedom it embodies are at the foreground because they are an essential part of dignity. I am not afraid of using highly evocative words – concluded Rodotà - “ I am convinced that a thorough analysis of the relationship between privacy and dignity, is fundamental to get a really firm grasp of man’s condition in this millennium and identify the pattern according to which democracy is being modelled”.

Various issues were then raised by the floor. Ermelando Cosmi addressed the core questions whether security is a threat to democracy, or, conversely, whether democracy is an impediment to security. Modern societies are facing a serious dilemma – noted Cosmi. “On the one hand,



public opinion wants policy makers to improve security, and, for obvious reasons, identification technologies are seen to play a pivotal role in world security. On the other hand, security policies lower citizens' fundamental rights and might even pave the way for future dictatorships". Cosmi concluded that surveillance is not inherently sinister or malign. But the focused attention to persons and populations with a view to influencing, managing or controlling them - that we call 'surveillance' - is never innocent either. Cosmi's worries were largely shared by Rodotà who emphasized that the growth of biometric technology can change the nature of our open and mobile society into a society where the right to disappear could be dramatically reduced. Prof. Rodotà cited a public debate about the introduction of electronic identity cards occurred some years ago in France. During this debate a man took the floor and said: "I was living in Paris during the Nazi occupation. I had the opportunity to falsify identity cards of Jewish people, and I saved more than thousand people in such a way. Are you aware that if Nazi used electronic identity cards all these Jewish people would have been doomed?" It's not a problem of identification concluded Rodotà - the society can decide that we need more secure identification systems, but this cannot be done regardless to the right to decide on your body, on your health, on your physical liberty. We should be cautious and capable to respond to the attacks coming from terrorism; above all, we should be brave and never forget our past, which reminds us of insufferable forms of authoritarianism. We are actually in danger of being exposed, once again, to authoritarian measures. Democracy is a valuable good, but it is fragile and should not be taken for granted once and for all.

Rodotà's perspective was partly contested by Kush Wadhwa. Mr Wadhwa observed that for a bit of convenience, we all give up our privacy rights on a regular basis (computers, mobile phones, credit cards, etc). This is a rational trade off between convenience and the right to be let alone. Biometrics is not the main threat to privacy rights and it can be even used as a privacy enhancing technology. Undoubtedly biometrics – as any other technological innovation - may imply some political risks, but humanity has always faced risks, and there has always been a debate about how to manage them. Today, unlike in the past, risk is seen not as something we can handle or perhaps even turn into opportunity, but as something that we suffer from and must be guarded against. This has now become one of the major barrier to social, scientific and technological advance - concluded Mr Wadhwa.

Finally Emilio Mordini raised the issue of human experimentation to test biometric technology and other IT Security Technologies. Mordini noted that biometric devices need to be tested in small populations before being used in larger trials. We presume – stated Mordini – that most, probably all, biometric technologies are safe and innocuous. Yet we should consider both their level of



psychological intrusiveness and their potential to extract sensitive data from the enrolled subjects. Mordini thus advocated an ethical scrutiny of human experimentation in the field of biometrics and asked Rodotà – as a member of the EGE – to address the issue of the ethical rules to be followed in the ethical review of such experiments.

The morning session was then concluded by Kush Wadhwa's presentation. He started his speech by outlining the difference between two kinds of identification: identity can be defined by what we HAVE (namely by what we carry with us or what we know; e.g., ID, microchips, PIN, etc) and it can be defined by what we ARE (namely physical and behavioral features; e.g., fingerprints, iris, retina, hand, face, voice, etc). There are many different ways to look at identity, one of them is that there are plural identities. "I am Kush the father, the husband, the scholar, the professional – observed Mr Wadhwa - We all have many different identities and we function differently in those identities. Things like ID, chips and etc. are things related to something that we HAVE as opposed to biometrics which is not something we have but something we ARE. It's an essential difference between biometrics and the things we were talking about this morning which are things like RFID, implantable chips or anything else that are not biometrics". The big difference between any other identification system and biometric systems is that a password is either right or wrong; on the contrary biometric data have different possibilities of match. It means that biometric identification is probabilistic. Another important difference is that biometrics works from images to templates. Fingerprint image, for instance, is converted into bar codes, ones and zeros: that is a template. Storing only templates safeguards privacy because, while there is always the possibility to go from an image to a template, there is no way to go from a template to an image. Wadhwa argued that it is common belief that biometrics can solve the problem of identity. That is incorrect. For instance biometrics cannot solve the problem of identity path or identity management. "I ask Emilio to give me his fingerprint and he tells me his name is Emilio Mordini – said Wadhwa - I attach that fingerprint to Emilio Mordini and all other relevant information that he gives me. That biometrics is forever imprinted and linked to that particular piece of information. He could have told me that his name was Kush Wadhwa!". Wadhwa continued that "in the UK there is a large debate on national ID cards. The process of getting to a national id card is an important one. Why? Because before you can have a national id card related to a biometrics you first need to establish identity of people. How are you going to do that? A way to establish the identity of people is to ask them to show things like their birth certificate; another way would be to go to the office with a witness. Those are all different identities by which people are identified". This is the very reason – argued Wadhwa - why biometrics can be used to preserve anonymity. "What is happening in the US – add Mr Wadhwa - is that you don't actually have to give a personal information to get a medical exam and that can



be accomplished by biometrics. In some AIDS screening programs they invite you to give an iris imprint with a sample of your blood. They will collect no personal information, they have no idea who you are. The only way to collect the result of your test was to resubmit and verify against your iris imprint and get results of your test. This way you get no personal information and yet you are able to make medical transaction". Biometrics can affect privacy in two ways: it can erase privacy if used for other purposes than originally intended, by linking different data, or if data are captured without informed consent; but it can also protect privacy providing access to sensitive data, allowing individual control over personal information and protecting against identity fraud. Wadhwa's point was that biometric technology has the potential to make security systems more democratically accountable and amenable to ethical scrutiny.

Wadhwa noted that when the Internet was coming out, in the early 1990, there were no Internet privacy laws, no rules. People thought that the Internet would incur to our privacy to such a great extent that we would have no privacy anymore. The amount of misinformation that existed related to privacy in Internet was extraordinary and this is case today when it relates to biometrics. It is an extraordinary amount of misinformation related to biometrics and privacy. There are so many information out there that are just incorrect. For instance – said Wadhwa – it is incorrect that biometrics can by itself solve many security problems. People believe that biometric solutions will solve the problem of terrorism: clearly that is not true because terrorism is a very complex problem in which identification problems play only a minor role.

Obviously Mr Wadhwa did not deny that biometrics may raise some privacy concerns, but he suggested that they should be addressed proactively. According to Wadhwa there are two main privacy concerns: a concern referred to PERSONAL privacy, in which users object to provide biometric data because biometrics is perceived to be used for profiling, and this is usually concentrated within certain cultures, nationalities or classes; the other concern refers to INFORMATIONAL privacy, in which the users fear a data misuse or a function creep, or a misuse of associated non-biometric data. Mr Whadwa outlined a framework to evaluate the relationship between privacy and biometrics. To evaluate the relationship between biometrics and privacy (IBG's BioPrivacy) three steps are necessary: because not all biometric deployments bear the same privacy risks, the first should be an evaluation of the application; the second is related to the extra precautions certain technologies require, so there is a need of technology risk rating; the third step should include BioPrivacy best practices. To evaluate a biometric application, K. Whadwa then suggested a checklist to test the degree of privacy invasiveness of an identification system. As technologies improve and markets change, potential privacy invasiveness of technologies can also change. There are some main central considerations in biometric



technologies referring to verification/ identification, overt/covert, behavioral/ physiological, interoperable/closed, for which these technologies are rated LOW (few privacy issues) MEDIUM (limited potential misuse of technology), and HIGH (moderate risk of privacy). For example facial recognition or fingerprint should be rated high, iris recognition can be considered medium and hand geometry, signature and speaker verification can be regarded as LOW risk technologies.

In conclusion Mr Whadwa gave his message: while many industries are afraid that privacy experts inhibit the growth of biometric industry, he thinks that this is the challenge that can prop up biometric industry, through the constant search of always more and more secure, safe and reliable technologies.

A discussion followed Wadhwa's presentation. Many participants took the floor (van der Ploeg, Romano, Mordini, Cosmi, Frischholtz, Chadwick, Bicz). The debate chiefly focused on privacy invasiveness of various biometric technologies. Mr Wadhwa judged biometric identification technologies based on behavioral features (e.g., voice, signature, key stroke dynamics, walking, etc) to be less invasive because they are less accurate. Yet Mordini argued that identification based on behavioral features can disclose sensitive information, not excluded medical information. Wadhwa contested this statement, his central argument was that the purpose of biometrics is either to verify or to identify, it is not to obtain health information. Of course there is always the risk of misconduct but this risk is not higher with biometrics than with any other technology. Actually it is something that has not to do with biometrics– concluded Wadhwa – but with the civil and political ethos.

The afternoon session was opened by Mario Savastano who began his presentation by stating that biometric techniques represent one of the most sophisticated technologies currently available on the market. Biometric technology responds to a generalized request of increasing security measures, as logical and physical access control, in critical sectors. At the same time, he highlighted that, unfortunately, a correct and moderated implementation of biometrics still requires the resolution of several heterogeneous problems. The market today is more mature to deal with biometrics, but there are still some technical and non technical factors in biometrics that need to be properly addressed. Technical factors are uncertainty and vulnerability of the systems; non technical factors are related to privacy and accessibility issues, which are the real challenge on the road of biometrics, because they may differ from country to country, and also in the same national context, and they may vary according to the application and the normative applied.



In Savastano's opinion, the scarce consideration of non-technical issues may be considered as one of the matters of the unsatisfactory diffusion of biometrics. The potential for negative social consequence of biometrics should not be overestimate, argued Savastano, nevertheless they should be taken seriously. As far as direct medical implications of biometrics are concerned, Savastano argued that, realistically, they are almost non existent. No biometric technology has the potential to be unsafe. Yet people's concern should be honestly considered and addressed, even if it is largely irrational. As far as biometric technologies are used in the society at large, one should involve in their application consumers' associations, trade unions, citizens' groups, etc. Indirect medical implications regards the possibility to infer medical information from biometric data. This possibility cannot be completely excluded but it is – in Savastano's opinion – quite remote. However also the risk of indirect medical implications should be taken seriously into account and properly addressed.

Accessibility represents the second non-technical factor that must be satisfied for a correct and harmonic diffusion of biometrics. Savastano mentioned the definition of accessibility referred to computer systems in the Italian law: "the capability of computer systems, in accordance with the attained technological knowledge and its limits, to supply services and to provide information which can be availed of, without discrimination, also by those who need supporting technologies or special configurations because of some disability". "Supporting technologies" are the tools and the technical hardware and software solutions that enable disabled users to overcome or reduce the initial disadvantages in accessing the information and the services supplied by computer systems. Accessibility in biometrics has two aspects: age and disabilities. For instance, as fr as fingerprints are concerned, elderly, as well as infants, have a problem in being enrolled by existing fingerprint scanners because of the height of their papillary relief. In infants and small children the height of the papillary relief increases according to the growth of the body. The elderly, on the other hand, may experience a deterioration of their papillary relief. This means that for most fingerprint scanners, this "decrease in the quality" of the biometric characteristic may lead to a decrease in the quality of the scanned image and to unpredictable diminished possibility of correct identification.

In the case of iris scanning, a medical research found that cataract surgeries may change iris textures in such a way that iris recognition systems may detect these differences with associate false rejection problems, so in some cases the users have to re-enroll. Concerning the age of the users, for many biometric technologies it should be possible to identify what Savastano called a "golden window".



Some more accessibility problems may be the absence, or a non useful or unstable physical body part (e.g., blind people, mutilates, etc); or behavioural features required for the correct operation of a biometric technique or the inability to access (e.g., wheelchair, Parkinson's disease, etc), or difficulty in accessing to the biometric sensor or user terminal or even the inability to understand the instructions, or recall the correct procedures (e.g., mild dementia, deaf people, illiterates, etc.).

The countermeasures proposed by Savastano for these problems are based on a central requirement: any biometric system should be easily accessible to all subjects and should not disadvantage any subject. The operator/designer should take into account disabilities, inabilities and problems of subjects operating a system. Some people in the floor suggested that multi-modal biometric system could solve accessibility problems. Savastano was quite sceptic about this solution, because multi-modal systems may only address disability problems but not age-related problems. Mr Bicz (OPTTEL) suggested the use of ultrasound systems, which work with higher resolution, to address age-related problems, but Savastano objected that biometric ultrasound systems are still very expensive.

A discussion followed, where some participants (Mordini, Grondin, van der Ploeg, Romano, Bicz) objected that Mr Savastano seemed to underestimate risks of data misuses, e.g. collecting health or medical information, detection of mental retardation or dismorphysm. They both pointed out that biometrics can have unintended consequences that include reinforcing forms of social control. An important dimension of the technological aspect of surveillance practices is that seeking superior technologies appears as a primary goal, noted Dr Grondin. The kinds of technologies sought for security purposes - iris scans, face-recognition, smart cards, DNA - rely heavily on the use of searchable databases, with the aim of anticipating, pre-empting, preventing acts of terrorism by isolating in advance potential perpetrators. The increasingly automated discriminatory mechanisms for risk profiling and social categorizing represent a key means of reproducing and reinforcing social, economic, and cultural divisions in informational societies. Database marketers in the USA use crude behavioral categories to describe neighbourhoods, such as 'pools and patios' or 'bohemian mix', and CCTV operators in the UK target disproportionately the 'young, black, male' group. Categorical suspicion has consequences for anyone, and it is already clear in several countries that 'Arab' and 'Muslim' minorities are disproportionately and unfairly targeted by these measures.



All these issues will be addressed in the next BITE meeting that will be held in Geneva on July 8th 2005 and that will be devoted to biometrics and migrants. Therefore concluding the current meeting, Dr Grondin invited all participants to join the BITE consortium in Geneva.



2nd scientific BITE Project Meeting - 26th April 2005 CNR Italian Research Council

Ever since the Magna Charta to the Charter of Fundamental rights of the EU, the respect for the body and for dignity have been basic components of the human being and have been fundamental conditions for freedom and equality. The evolution of information technology is likely to result in intimate interdependence between human bodies and technology. As biometric identification devices become more pervasive, they may compromise privacy in a deep and thorough fashion: they can reveal more about a person than only his identity.

The overall aims of the meeting are:

1. to review the scientific evidence of biometrics with particular reference to privacy;
2. to review implementation of existing law and policies and to formulate policy options;
3. to fulfill a prospective role, anticipating the major reasons for concerns surrounding biometrics and privacy, and providing early warnings for new ethical, legal, and social issues;

After a presentation from each expert, the experts will be questioned by the chairman and the panel. Experts will witness on specific questions related to the following issues:

- Is the use of biometrics compatible with personal privacy?
- Biometric, security and respect for the person: is biometric the new panopticon?
- Biometrics and privacy: current challenges, policy options and level of governance
- Can privacy be safeguarded in people who are unable or less able to give an informed consent to the use of biometrics?
- Can biometric patterns be linked to behavioral characteristics, or predispositions to medical condition? Under what circumstances can biometric data be misused?
- In what situations of bioethical relevance do the potential risks of biometric usage outweigh the benefits?

**2nd scientific BITE Project Meeting - 26th April 2005****Participant List**

Name	Affiliation	Mail Address	Email
Anaclerio, Michele	Italian Ministry of Defense	Via Santo Stefano Rotondo n. 4 00184 Roma - Italy	michele.anaclerio@tiscali.it
Balestrieri, Valeria	Centre for Science, Society and Citizenship	Via Sistina, 37 - 00187 Roma - Italy	v.balestrieri@bioethics.it
Bastianon, Vittoria	Centre for Clinical Research and Bioethics	Viale Regina Elena 324 - 00161 Roma - Italy	perinat@flashnet.it
Bernardini, Mario	Associazione Stampa Medica Italiana	Via Valpolicella 19 00141 Roma - Italy	numedi@tiscalinet.it
Bicz, Agnieszka	OPTEL	ul. Otwarta 10a PL-50-212 Wroclaw Poland	a.bicz@optel.pl
Bicz, Wieslaw	OPTEL	ul. Otwarta 10a PL-50-212 Wroclaw Poland	w.bicz@optel.pl
Bisogni, Francesco	Centre for Clinical Research and Bioethics	Viale Regina Elena 324 - 00161 Roma - Italy	francesco.bisogni@libero.it
Cosmi, Ermelando V.	Centre for Clinical Research and Bioethics	Viale Regina Elena 324 - 00161 Roma - Italy	Ermelando.cosmi@uniroma1.it
Calicchia, M.Cristina	Italian National Institute of Health	Istituto Superiore di Sanità Viale Regina Elena 299 00161 Roma - Italy	cristina.calicchia@iss.it
Cecchinelli, Giancarlo	ESA Communication	Piazza Campo Marzio 45 00186 Roma - Italy	g.cecchinelli@esacommunication.com
Chadwick, Ruth	Centre for Economic and Social Aspects of Genomics	Lancaster University Furness College Lancaster LA1 4YG United Kingdom	r.chadwick@lancaster.ac.uk
Cinti, Caterina	University of Siena	Via Tommaso Pendola, 62 - 57100 Siena - Italy	ccinti@area.bo.cnr.it
Frischholz, Robert	HumanScan	Wetterkreuz 19a	r.frischholz@humanscan.de



		D-91058 Erlangen Germany	
Grondin, Danielle	International Organization for Migration	17, Route des Morillons CH-1211 Geneva 19 Switzerland	dgrondin@iom.int
Keller, Flavio	University Campus Bio- Medico	Via Emilio Longoni, 83 - 00155 Roma - Italy	F.Keller@unicampus.it
Mordini, Emilio	Centre for Science, Society and Citizenship	Via Sistina, 37 - 00187 Roma - Italy	e.mordini@bioethics.it
Ottolini, Corinna	Centre for Science, Society and Citizenship	Via Sistina, 37 - 00187 Roma - Italy	c.ottolini@bioethics.it
Petrini, Carlo	Italian National Institute of Health	Istituto Superiore di Sanità Viale Regina Elena 299 00161 Roma - Italy	carlo.petrini@iss.it
Pratellesi, Marco	Corriere della Sera University of Siena	via Solferino 28 - 20121 Milano - Italy P.zza san Francesco, 8 53100 Siena - Italy	MPratellesi@rcs.it
Rodotà, Stefano	University La Sapienza		rodota@garanteprivacy.it
Romano, Giuseppe	Il Domenicale	V. Senato 12 20100 Milano - Italy	giusepperomano@ildomenicale.it
Savastano, Mario	Federico II University of Naples	Via Claudio 21 - 80125 Napoli - Italy	mario.savastano@unina.it
Tittoni, Rita	ESA Communication	Piazza Campo Marzio 45 00186 Roma - Italy	r.tittoni@esacommunication.com
Van der Ploeg, Irma	Institute for Healthcare Management & Policy	PO Box 1738 3000 DR Rotterdam Netherlands	vanderploeg@bmg.eur.nl
Whadwa, Kush	International Biometric Group	Devonshire House 1 Devonshire Street London, W1W 5DR United Kingdom	kwadhwa@biometricgroup.com