SYNESIS
A JOURNAL OF SCIENCE, TECHNOLOGY, ETHICS, AND POLICY

Combining Internet Computing, Biometrics and Sensors to Leverage Deterrence

David J. Smith[1]

1. Ilia State University, Tbilisi, Georgia, Email: dsmith@ripleylane.com.

Abstract

Deterrence is a concept much more ancient than the Cold War and far broader than mutual assured destruction – MAD – which came to characterize the standoff between the United States and the Soviet Union. The requirements of deterrence will vary, however, excellent knowledge and intelligence about the opponent will always be necessary. Deterrent calculations must take into account not only the cultural context and decision making procedures of the other side, but also multiple personalities, agendas, relationships and group dynamics. Consequently, psychological profiling from afar has become a mainstay of intelligence analysis. Developing computer technology, including the boom in mobile devices, can help gather information, process and analyze it and deliver messages to target audiences. For the first time, someone with the right tools can reach into the office, car, medical facility, bedroom, and even bathroom to collect information and deliver targeted messages back to the same. Gathered and analyzed properly, such information could be a real boon to extending influence, including deterrence. Of course, this raises a plethora of legal and ethical issues that must be seriously examined. Nonetheless, the technology is out there.

Keywords: deterrence, psychological profiling, hypertargeting, intelligence

We are at one of those moments in the course of human events when a number of bounding technologies are coming together – computers and computing, including mobile computing, neuroscience, biometrics and sensors. When I say computers and computing, I mean the computational capabilities of the machines, the computations that make the machines useful as well as advances in networking such as increasing available bandwidth and decreasing bandwidth requirements. In addition, since the end of the Cold War, there have been heartening developments in analysis of the concept of deterrence.

Deterrence, I suspect, is at least a million years old. When, for the first time, a primitive human raised a club toward another but did not use it, he made a deterrent calculation that was at once simple and complex: "I would not want my skull bashed in with this thing and my guess is that you would not want that either." He could see in his opponent's reaction whether deterrence was working. There was no effete analysis. He had the capability and demonstrated will and he was thoroughly prepared for deterrence to fail. If, for whatever reason, his opponent persisted, he would use the club to bash his brains out. And anyone within earshot would take heed. Modern analysts take notice.

It probably went something quite like that, although we have no evidence of it. However, we do begin to have written records of deterrence, successful and unsuccessful, with Thucydides, 2,400 years ago. By the time of the

Peloponnesian War, however, culture had become quite complex and Thucydides records discussions reminiscent of our own time – assumptions about what would and would not work; signals understood and misunderstood. In the Battle of Corcyra, for example, the Athenians wanted to deter Corinthian aggression against their ally, Corcyra, without a fight. Accordingly, they sent a token fleet and chose as one of its commanders a man with family ties to Sparta. But the Corinthians, Sparta's allies, could not have known whether there were more Athenian warships in the next bay, and if anyone noted the heritage of the Athenian commander, there is no extant record of it. A war that changed the Greek world forever ensued (1,2).

Deterrence is a concept much more ancient than the Cold War and far broader than mutual assured destruction – MAD – which came to characterize the standoff between the United States and the Soviet Union. Regrettably, more than two decades after the end of the Cold War, much discussion about deterrence still revolves around MAD. Here is one personal example. I was recently asked to write a chapter about the prospects for cyber deterrence. After a brief introduction that cited Thucydides and Livy, I wrote, "Could Cold War-style mutual assured destruction – MAD – work against cyber weapons? In a word, no."(2) The remainder of the chapter raised what I thought were quite clever considerations about the concept of deterrence as it may or may not apply to cyber conflict. Consequently, I recommended a change in chapter title. But the original tag persisted into print: "Cold War Paradigms: Does MAD Work with Cyber Weapons?" (2)

Our fixation with Cold War deterrence is altogether unwarranted. The Cold War occupied just over four decades of human history. Moreover, MAD was unsophisticated and mostly wrong. The American concept of nuclear deterrence, which developed into MAD, stemmed from economics and game theory, with little regard to Soviet thinking. There was scant perceived need to dwell on what anybody thought in Russia. Thomas Schelling, the intellectual father of Cold War deterrence explained, "You can sit in your armchair and try to predict how people will behave by asking how you would behave if you had your wits about you. You get, free of charge, a lot of vicarious, empirical behavior." (3)

This sort of thing was turned into policy. As Fred Kaplan explains, "McNamara's Whiz Kids calculated that the Soviets would be sufficiently deterred if we could kill 30% of their population and destroy half their industrial capacity (4). Such reasoning was not only a priori; it was deduced from only half of the relevant information.

One of the earliest criticisms of this approach came from Graham Allison's analysis of the Cuban Missile Crisis or, more precisely, analysis of the American decision-making process during that incident. The lone rational actor sitting in an armchair did not fit with Allison's observations. Consequently, he offered two more models that he called "organizational process" and "governmental politics"(5).

Although we say colloquially things like, "France decided" or "Washington believes", nations and cities do not decide or believe anything. Such phrases are shorthand for the action of some group of decision-makers in each polity. Who they are and how they operate varies from country to country, organization to organization and time to time. Not only will decision-making in the United States differ from decision-making in Pakistan or in al Qaeda in the Arabian Peninsula, it will vary from administration to administration, especially on major issues.

In complex modern democracies at least, it is unlikely that a decision will be made entirely by one person. Although the legal authority to decide may reside with one person, that person is likely to be surrounded by other senior officials and advisers, formal or informal, as important decisions are made. That means that deterrent calculations must take into account not only the cultural and procedural contexts of the other side, but also multiple personalities, agendas, relationships and group dynamics. Outside the decision-making room, diplomatic cables zip around the globe, the 24-hour news cycle grinds on and politicians proclaim and posture. In this light, Allison's two new models made a lot of sense.

With the end of the Cold War, Americans began paying attention to a much broader array of situations than they had since World War II. Furthermore, American scholars gained access to some Soviet archives (6,7). They found out that we had deluded ourselves with MAD. In reality, the Soviets had viewed unacceptable damage very differently than we. Under certain circumstances, they had been prepared to ride out a nuclear war, believing that victory was possible (6,7). By the way, it also turned out that Nikita Khrushchev, Soviet Premier during the Cuban Missile Crisis, did not run a decision-making process similar to that of US President John F. Kennedy. Apparently, he pretty much sat alone in his room, minding his own counsel and issuing orders (6,7).

How the other side makes decisions is important for deterrence. Are we trying to affect the behavior of an individual, a small group or a large group? Are there members of the group who hold sway over the group or part of it? What the other side thinks and holds valuable also matters. The other side believing that losing 30% of the population could be acceptable presents a very different deterrence challenge than it believing unequivocally that this would be unacceptable. To return to our primitive human, a foe who actually wants his head bashed in is very different from one who would prefer to avoid that fate. Perhaps martyrdom-seeking *jihadis* have finally convinced western thinkers that Schelling's armchair approach to deterrence just will not work.

Keith B. Payne underscores the importance of even whacky personal idiosyncrasies. In the 1983 Beirut barracks bombings, 241 American and 58 French military personnel were killed by two truck bombs. Nearby Italian participants in the same mission were spared (8). Syrian Defense Minister Mustafa Tlas explained that he had instructed Lebanese insurgents to spare the Italians because of his love for actress Gina Lollobrigida (7). To update the idea – imagine if we were to find out that Kim Jong-un is obsessively downloading Miley Cyrus videos!

In a step toward operationalizing what should have been common sense observations, Payne developed a framework for analyzing, to the extent possible from afar, how an opponent makes decisions and what things that culture values (7). Excellent knowledge and intelligence are requirements of deterrence. No matter how determined we demonstrate ourselves to be and how awesome our threats, there is no substitute for knowing the mind of the opponent or opponents.

In the old days – meaning the pre-Internet era – under the best of circumstances, intelligence analysts kept files of every shred of information they could gather on anyone who might someday matter – newspaper clippings, conference speeches, photographs and reports from encounters with counterparts, diplomats or business people. The resulting profiles were fragmented, often based on single encounters with untrained observers.

Psychological profiling from afar, arguably more an art than a science, became a mainstay of intelligence analysis during the Cold War and beyond. Detractors said that accurate diagnoses were impossible with shreds of information and without direct contact with the subject. Nonetheless, American decision-makers were as informed as possible about foreign leaders and prepared to encounter their psychological traits. Though less than ideal, this was better than being unprepared or, worse, mirror-imaging about the motivations of foreign leaders, particularly the nasty ones.

Psychologist and journalist Daniel Goleman illustrated the tension between the ideal and the possible in a 1991 *New York Times* article, written just as Operation Desert Storm got underway. Jerrold Post, a George Washington University psychiatry and political science professor and former chief profiler for the CIA, labeled Iraqi President Saddam Hussein a malignant narcissist in open Senate testimony (9). This naturally sparked a debate over the value psychological profiles drawn from afar. Otto Kernberg, a Cornell psychiatry professor who had pioneered the diagnosis of malignant narcissism, said that he could not attribute it to Saddam because he did not know enough about him (9). Robert Jervis, an international relations professor at Cornell chimed in, "Psychoanalyzing someone from a different culture from a distance is very hard."(9)

Post, Goleman wrote, "Drew on a wide variety of sources, ranging from the half dozen biographies of Mr. Hussein and his speeches, to interviews with people who have had personal dealings with him."(9) That was what was available in 1991. Today, however, computers can revolutionize the concept of psychological profiling from afar, which could be a boon to effective deterrence. Post and his successors could now have access to more data than they could have dreamed possible just two decades ago; in some respects, more data than face-to-face interviews might have revealed.

Developing computer technology, including the boom in mobile devices, can help gather information, process and analyze it and deliver messages to target audiences. There is a lot more data to process but there is also so much more capability to process it. Most important, for the first time, someone with the right tools can reach into the office, car, medical facility, bedroom, perhaps bedrooms, and even bathroom to collect information and deliver targeted messages back to the same. A look at what is going on in online commerce affords a good glimpse of the rapidly developing future.

What I am about to say raises many legal and ethical issues that must be examined and I am not here advocating any

course of action, certainly not without full consideration of matters legal and ethical. However, if maximizing the effectiveness of a deterrent strategy depends on knowing as much as possible about the individual or group to be influenced, these technologies are becoming available.

Let us begin with two facts. First, there are about two and a half billion people connected to the Internet. Just about anyone of interest in considerations of deterrence is connected. Second, there are about seven billion mobile computing devices in the world (10,11). Meanwhile, cookies – little text files that reside on your browser to log your website visits and even your website interactions – are on their way out. They don't work on mobile devices, they are succumbing to "do not track" features offered on many browsers and they are being supplanted by proprietary replacements such as iOS AdID and VendorID (12,13).

However, cookies are the mainstay of E-commerce. Their impending demise has not diminished businesses' appetites for hypertargeted advertising; it set them on a search for new, better tools. This has led to the development of behavioral tracking, mobile signatures and device matching. The objective of device matching is to determine that the same user is associated with, say, a PC, a tablet and a smartphone. One company, Drawbridge, "…uses an algorithm to determine whether a user on a mobile device and a PC is the same person based on information such as location, IP addresses and browser type" (14). Drawbridge, according to its founder, has already matched more than 500 million users across devices. Its accuracy rate is between 60% and 90% (14). The business application is clear. If a user checks out flights to Rome on an iPad in the morning, he or she could receive targeted advertisements about travel to Rome on a PC or smartphone throughout the day.

Of course, the business of business is to sell. In general, business does not want legal issues or bad press, so its interest in tracking – it even does not like this word – is directed at information that is useful for selling products or services. So, an online targeting specialist may be able to tell you that an unnamed individual lives in a particular area, works in another, is associated with four devices, that he or she appears to fit a certain demographic category, is concerned about high blood pressure and is interested in flights to Rome. Companies marketing these technologies steer clear of trying to identify a particular user (14,15). That is already a lot, and the typical advertiser has little interest in pushing his or her curiosity farther. The objective is to target advertising – Rome hotels or a new blood pressure medicine, for example – not to pry into every psychological detail.

Furthermore, businesses must consider return on investment. Hypertargeted advertising is an investment, not an intellectual puzzle for computer scientists. Do you need to know that a potential customer is at this moment in a particular grocery store? Or would it have sufficed to know that over the last few days, he or she has been Googling carpet stain removers? Does the increment in the cost of additional information result in a greater increment in sales revenue? Or, to take the example of device matching presented above, how much is it worth to raise the accuracy rates of 60% to 90% or the 90% to as close to 100% as possible? All that is at stake is that the nth customer interested in carpet cleaner may fail to view a targeted advertisement and a person with hardwood floors may see it and ignore it. The overall objective of the advertiser may well be met at the lower cost.

A relevant case in the news is the recent announcement by Ken Rudin, chief of analytics at Facebook, that the social media giant will track users' cursor movements (16). If successful – and that means not only tracking the cursor movements, but storing and exploiting all that data – Facebook might be able to tell an advertising executive, for example, that a user hovers over certain kinds of advertisements but never clicks (17). A computer scientist may seize upon the challenge for its own sake, but the ad executive will want to calculate return on investment.

Some techniques will pan out and others not. However, the bottom line is that business is driving computers and computing toward gathering, analyzing and exploiting ever more social data. Sullivan McIntyre, an executive with Salesforce, a company that bills itself as "the leading social media marketing suite," concludes, "It becomes increasingly possible to make guesses about future behavior." (18)

However, what if the tracker is not a Rome hotelier or a cleaning solvent manufacturer but a hostile individual, organization or nation-state, unconcerned with lawsuits, bad press or, at least to a point, return on investment? Now, to the commercial tracking techniques, add spyware like Flame or Georbot. With the right tools, a tracker could read E Mails, take screen shots, turn on the target computers' cameras and microphones, check for other hosts on the target networks and make a diagram of the

target's social and business networks (19,20). He or she can observe intimate details of family life, personal habits, social connections, licit or illicit, medical and financial records and more.

To achieve some of this, one might need some fairly advanced spyware like Flame, which was likely developed by a well-resourced nation-state (21). However, the advent of Georbot – apparently sponsored by Russia but run by a known hacker – probably indicates that the price of entry for such spyware is already falling (22). Furthermore, today, anyone can download an application that will assemble and display a target's associations and contacts. According to its website, "Maltego is a program that can be used to determine the relationships and real world links between people, groups of people (social networks), companies, organizations, web sites and Internet infrastructure."(23) Enter, for example, an Internet Protocol address, and in a matter of minutes, Maltego will create a diagram of all associations with that address.

Finally, let us add advances in sensors and biometrics. With its usual fanfare, Apple a few weeks ago introduced its latest smartphone, the I-Phone 5S, which features a fingerprint identity sensor. Instead of entering a four digit PIN to access your I-Phone, with the 5S, you can simply place your finger on the screen. Frankly, that is nothing. Today, you can use your smartphone to measure and record vital signs like heartbeat, blood pressure or glucose levels.

Access the Apple I-Tunes App Store and check out, for example, an application called Blood Pressure Manager. "Have you ever wanted to have a single app to track all of your health and medical readings," the app's promotional statement asks? You can even upload all your medications to monitor how your vital signs react to them. Diabetes App affords another example. With this app, you can record your daily food and liquid intake, glucose levels, injections, medications, exercise and much more. The app even creates charts out of all this data so that the user can observe trends.

Or, consider Scanadu. "Send your smartphone to med school…" proclaims its website. Scanadu is "A scanner packed with sensors that enables anyone to conduct sophisticated physical exams – in a snap." (24) The Scanadu Scout is already on the market. Just touch its sensor to your temple and in seconds it will measure heart rate, body temperature, oximetry, respiratory rate, blood pressure and electrocardiography – all displayed on your smartphone. Coming soon is Scanaflo, which will, again according to its website, "Test for levels of glucose, protein, leukocytes, nitrates, blood, bilirubin, urobilinogen, specific gravity, and pH in urine."(25) It will also test for pregnancy. This company has realized the "tricorder," popularized in the television and film series *Star Trek* (25).

A final example is the controversial *23andMe* DNA analysis service (26). Until recently discontinued by the United States Food and Drug Administration (FDA), the company had offered a $99 "Spit Kit." Spit, seal and send, and your profile for 240 health conditions and traits would appear on your own personal webpage. *23andMe* provided so much data that one reviewer remarked, "I still haven't had the chance to read even half of it" (27). Such medical information, provided by a commercial direct-to-consumer source, also incurs a host of problems. *23andMe*'s failure to address these issues despite repeated FDA warnings ultimately led to the sanctions (28).

To a person suffering from high blood pressure or diabetes, someone who lost a parent prematurely to a congenital condition or to an anxious parent, these apps are useful tools, maybe even lifesavers. However, potential risks are not limited to the medical and ethical realm. Additionally, such databases provide fountains of personal information. If a tracker could hack into the mobile device on which these apps are used or the server on which the app company stores this data, or intercept the communications between them, he or she could harvest a wealth of medical data. An intrusion into a doctor's office or hospital network would complete the picture.

Let me conclude by offering a hypothetical profile that could today be developed on a person of interest. Country X and Country Y have been at loggerheads for years, the underlying geopolitical rivalry exacerbated by Country Y's activities in a field that Country X regards as particularly menacing. General Z is an important figure in Country Y's government, known to be part of the Leader's inner circle. On the surface, Z appears to be a normal product of his culture and loyal to the Leader. However, we now know the following. Z's relations at home appear to be cordial but not warm. He and his wife have separate bedrooms. In addition to his wife, he has a 13 year-old daughter and a 16 year-old son. The girl often laments the traditional strictures of her country's culture, often antagonizing her mother. The boy shows signs of some kind of substance abuse. Z frequently arrives home after

midnight but seldom stays at the presidential palace after seven. Z has high blood pressure and a worsening case of type II diabetes. His contacts to his doctor have been increasing. Every morning, he surfs western press sites, but only on one iPad, usually at a café where he stops on the way to work. Most of his routine contacts appear to be normal for someone in his government position and social status, except for two. One frequent contact is one of his university professors who is known to harbor somewhat dissident views. Another is an unknown person with whom he exchanges cryptic but frequent SMS messages. Both these people are contacted only on a second, personal smartphone. Z is an infrequent Facebook user, however, he does appear to have friended a number of Italians whom he met while on a one year graduate program in Rome years ago. Each year, his wife takes the children on holiday without him. Given his position, this may be because he is too busy to vacation, however, for the last two years, he has flown to Dubai for a week while the family was on vacation. Lately, he has been investigating flights to Rome. He always opts for the one-stop option although there are direct flights available. He enters 2 adults and 0 children in the dialog box. He has also visited the websites of several medical facilities in or near Rome.

Of course, this hypothetical profile is an ideal. In espionage, as in war, some degree of fog is inevitable. Building such a profile would require a high success rate on a high priority target with sophisticated resources. Nonetheless, there is nothing in the preceding paragraph that is beyond the reach of current technology. I shall leave it to the neuroscientists and psychologists to ponder what one could do with such a profile.

Suffice it to say that gathering this kind of information could bring a target as close – or, in some aspects, even closer – than a patient in a psychologist's office. Gathered and analyzed properly, such information could be a real boon to extending influence, including deterrence.

Of course, to repeat what was said at the outset, this raises a plethora of legal and ethical issues that must be seriously examined. What kind of data may US agencies legally gather? Is it legal to collect only against foreigners, or can American citizens be targeted under certain circumstances? What kind of data can be collected on foreign leaders, and who is a foreign leader? These are just some of the legal and ethical issues that arise. Whatever answers emerge, the technology is out there and it is becoming more capable day-by-day.

References

1. Thucydides, Warner R, Finley M. History of the Peloponnesian War. Harmondsworth, Eng.: Penguin Books; 1972.
2. Smith D. Cold war paradigms: does MAD work with cyber weapons? In: Sample T, Swetnam M. (eds.) #Cyberdoc: no borders - no boundaries: national doctrine for the cyber era. Arlington: Potomac Institute Press; 2013. p. 99-121.
3. Archibald K, Deutsch M. Strategic interaction and conflict: original papers and discussion. Berkeley: Institute of International Studies, University of California; 1966.
4. Kaplan F. The wizards of Armageddon. New York: Simon and Schuster; 1983.
5. Allison G. Essence of decision: explaining the Cuban missile crisis. Boston: Little, Brown; 1971.
6. Payne K. Deterrence in the second nuclear age. Lexington: University Press of Kentucky; 1996.
7. Payne K. The fallacies of Cold War deterrence and a new direction. Lexington: University Press of Kentucky; 2001.
8. Beirut Marine barracks bombing fast facts. CNN [Internet] 2013 June 13 [cited 2013 Dec 17] Available from: http://www.cnn.com/2013/06/13/world/meast/beirut-marine-barracks-bombing-fast-facts/.
9. Goleman D. Experts differ on dissecting leaders' psyches from afar. New York Times [Internet] 1991 Jan 29. [cited 2013 Nov 11] Available from: http://www.nytimes.com/1991/01/29/science/experts-differ-on-dissecting-leaders-psyches-from-afar.html?pagewanted=all&src=pm.
10. CISCO. Cisco visual networking index: global mobile data traffic forecast update, 2012-2017. [Internet] San Jose, CA: Cisco Systems, Inc; 2013 Feb 6. [cited 2013 Oct 14] Available from: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html.
11. Internetworldstats.com. World Internet Users Statistics Usage and World PopulationStats. [Internet] [cited 2013 Oct 14] Available from: http://www.internetworldstats.com/stats.htm.
12. Brock J. Apple iOS 7 puts an end to unique device IDs. [Internet] San Francisco: AVG Technologies; 2013 June 18 [cited 2013 Oct 16] Available from: http://blogs.avg.com/mobile-2/apple-ios-7-puts-unique-device-ids/.
13. Learmonth M. A Google Cookie Replacement Could Upend Internet Advertising. AdAge Digital [Inter-

net]. 2013 Sept 19 [cited 2013 Oct 14] Available from: http://adage.com/article/digital/a-google-cookie-replacement-uproot-Internet-advertising/244241/.
14. Aquino J. Fingerprinting and beyond: the mobile ad targeting trade-off. AdExchanger [Internet] 2013 March 29 [cited 2013 Oct 14]. Available from: http://www.adexchanger.com/data-exchanges/fingerprinting-and-beyond-the-mobile-ad-targeting-trade-off/.
15. Miller CC, Sengupta S. Selling secrets of phone users to advertisers. New York Times [Internet]. 2013 Oct 5 [cited 2013 Oct 14]. Available from: http://www.nytimes.com/2013/10/06/technology/selling-secrets-of-phone-users-to-advertisers.html?pagewanted=all.
16. Rosenbush S. Facebook tests software to track your cursor on screen. Wall Street Journal [Internet]. 2013 Oct 30 [cited 2013 Dec 17]. Available from: http://blogs.wsj.com/cio/2013/10/30/facebook-considers-vast-increase-in-data-collection/.
17. Moscaritolo A. Report: Facebook test tracks your cursor movements. PCMAG [Internet] 2013 Oct 31 [cited 2013 Nov 10]. Available from: http://www.pcmag.com/article2/0,2817,2426602,00.asp.
18. Bloem J, Doorn M, Manen T, Ommeren E. Big social: predicting behavior with big data. Sogeti [Internet] Norway: Sogeti; 2012 [cited 2013 Nov 11] Available from: http://www.sogeti.no/upload/SV/Kalendarium/Dokument/Big-data2.pdf.
19. Aleks. The Flame: Q uestions and answers. Securelist [Internet] 2013 May 28 [cited 2013 Oct 14]. Available from: http://www.securelist.com/en/blog/208193522/.
20. Georgia: Russia responsible for Georbot cyber-spy attack. Infosecurity Magazine [Internet] 2012 Nov 1. [cited: 2013 Oct 14] Available from: http://www.infosecurity-magazine.com/view/29108/georgia-russia-responsible-for-georbot-cyberspy-attack/.
21. Nakashima E, Miller G, Tate J. US, Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say. Washington Post [Internet] 2012 June 19 [cited 2013 Dec 18]. Available from: http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.
22. Ragan S. Georgian CERT catches alleged Georbot on camera. SecurityWeek [Internet] 2012 Oct 31 [cited 2013 Dec 18]. Available from: http://www.securityweek.com/georgian-cert-catches-alleged-georbot-operator-camera.
23. Paterva. Maltego. [Internet] South Africa: Paterva, Ltd; [cited 2013 Oct 14] Available from: https://www.paterva.com/web6/products/maltego.php.
24. Scanadu. [Internet] NASA Ames, CA: Scanadu. [cited 2013 Dec 18]. Available from: http://www.scanadu.com.
25. Scanadu | Scanflow. [Internet] NASA Ames, CA: Scanadu. [cited 2013 Dec 18]. Available from: http://www.scanadu.com/scanaflo.
26. 23andMe. [Internet]. Mountain View, CA: 23andMe, Inc. [cited 2013 Oct 14]. Available from: https://www.23andMe.com.
27. Socrates. 23andMe DNA test review: it's right for me but is it right for you? Singularity Weblog [Internet] [cited 2013 Oct 14]. Available from: http://www.singularityweblog.com/23andme-dna-test-review-its-right-for-me-but-is-it-right-for-you/.
28. Gutierrez A. FDA: Inspections, Compliance, Enforcement, and Criminal Investigations- Warning Letters. 23andMe, Inc. [Internet] Silver Spring, MD: FDA; 2013 Nov 22. [cited 2013 Dec 28] Available from: http://www.fda.gov/iceci/enforcementactions/warningletters/2013/ucm376296.htm.