Usha Ramanathan

# Considering Social Implications of Biometric Registration

## *A Database Intended for Every Citizen in India*

The Aadhaar (Unique Identity) project has become the bane of average Indians, threatening access to all manner of services. Basic questions have been asked and never been answered. The Unique Identity (UID) project has been around for over five years. The Unique Identification Authority of India (UIDAI) was set up by an executive notification dated January 28, 2009, and came into its own after Nandan Nilekani was appointed as chairperson in July 2009 [1]. Now it has, as some observers say, become an experiment being conducted on the entire country.

In its early stages, the UID project was marketed, simply, as giving the poor and the "undocumented" an identity. It was to be voluntary, and an entitlement. But, it is evident even from the *Strategy Overview* document of the UIDAI that it was never intended to be an entitlement that people may choose to adopt or ignore [13]. The *Strategy Overview* said that "enrolment will not be mandated", but went on to add: "This will not, however, preclude governments or registrars from mandating enrolment" [2]. So, the potential for compulsion was built into the original architecture of the project. Starting in 2012, the voluntary aspect began to be eroded, and threats of exclusion from services and entitlements began to be bandied about. By January 2013, a virtual panic was set off when it was announced that various services and entitlements would not

KANNANSHANMUGAM,SHANMUGAMSTUDIO, KOLLAM /CREATIVE COMMONS ATTRIBUTION-SHARE ALIKE 3.0 UNPORTED

*Digital Object Identifier 10.1109/MTS.2015.2396113*
*Date of publication: 23 March 2015*

be accessible to persons who did not have a UID number.

Mr. Nilekani has said time and again that half the population was expected to be enrolled by the end of 2014; yet, there have been warnings that people without a UID number may find themselves unable to access benefits and subsidies if they do not have it – if a bank account had not been opened, and if the UID number were not embedded in the bank account. So, a subsidy for cooking gas, kerosene, and scholarships, for instance, became dependent on having a bank account seeded with the UID, or Aadhaar number.

From its inception, the UID project has been about creating the "database resident." The website of the Department of Information Technology, which has been renamed as the Department of Electronics and Information Technology, modestly carrying the acronym DeitY, has said all along that "Project UID, a Planning Commission initiative, proposes to create a central database of residents, initially of those above the age of 18 years" [3]. Yet the UIDAI has got even more ambitious and demanded that everyone, from the newborn to the oldest resident, be registered on its database. In actuality, it was always intended to integrate various databases to construct a profile of the Indian citizen: "the project envisages provision of linking of existing databases, as well as providing for future additions, by the user agencies" [3]. The MoUs between the UIDAI and various registrars that include the state governments, oil companies, banks, and the Registrar-General of India, who is in charge of census and the National Population Register and socio-economic and caste census, not only provided for various additional fields of data being collected during enrolment, but also for having the UID number appended to each respective database.

## Questioning Universality, Uniqueness, and Permanence in Biometric Collection

As for biometrics, documents reveal that when the decision was made to use fingerprints and iris for enrollment, there was no knowledge about whether such biometrics would work in India given the country's demographic and environmental conditions. In fact, it has since been found that with age fingerprints fade, that manual labor makes fingerprints difficult to read, that malnourishment-induced cataract blights an estimated 8-10 million people, and so on. The DG and Mission Director of UIDAI himself stated in November 2011: "The other challenge we face is the quality of fingerprints. Capturing fingerprints, especially of manual laborers, is a challenge. The quality of fingerprints is bad because of the rough exterior of fingers caused by hard work, and this poses a challenge for later authentication.... Issuing a unique identity will not be a major problem. But authentication will be, because fingerprint is the basic mode of authentication."

The UDIDAI collects face, fingerprint, and iris biometric data. The uniqueness of the UID number is said to be ensured by using the biometrics collected for "de-duplicating" the 1.2 billion plus resident population of India. That has always sounded like such an improbable task that it cannot do without some investigation of why the UIDAI thought they could pull it off. What did the UIDAI know about biometrics that gave it the confidence to roll out the project on a nationwide scale? The answer is, very little.

When the project got off the ground, and Mr. Nilekani took charge, among the early decisions taken seems to have been the introduction of biometrics. On September 29, 2009, the UIDAI set up a committee to review the state of biometrics in the country, and to suggest how they may be modified, extended, or enhanced to "serve the specific requirements of UIDAI relating to de-duplication and authentication." Interestingly, among its other tasks, the committee was asked to "obtain consensus (for) widespread propagation of biometrics in governmental and private sectors" [12]. Significantly, no other means of achieving uniqueness and de-duplication was suggested then, nor at any time since then; biometrics was the only tool.

> **The Unique Identifier project has become an experiment conducted on the entire population of India.**

The December 2009 report of the committee on biometrics was cautious [13]. The state of knowledge on biometrics was too meager. In its sample of 25 000 people, 2-5 per cent did not have biometric records. Globally, de-duplication accuracy of 99 percent had been reported from western populations, where there was good fingerprint quality and where the database was up to 50 million. To scale up the results from 50 million to a billion plus was fraught with uncertainty. And, importantly, there had been no study of fingerprint quality in the

Indian context. Indian conditions, the report read, "are unique in two ways: larger percentage of population is employed in manual labour, which normally produces poorer biometric samples. Biometric capture process in rural and mobile environment is less controllable compared to the environmental conditions in which western data is collected." It also found that if the way biometrics is captured is deficient, the "false acceptance rate" could be over 10%. The committee "strongly recommended that carefully designed experiments and proper statistical analysis under pilot should be carried out, to formally predict the accuracy of biometric systems for Indian rural and urban environments" (14).

As for the iris, it is technology of recent vintage, and, "compared to fingerprinting, iris capture is less studied and less standardised." So, the report tentatively suggested combining multiple biometric modalities, in this case fingerprint and iris. That was about all the committee was able to determine.

## Biometric Exceptions in a National Program as Big as India

Pursuant to this report, in February 2010, the UIDAI issued a "notice inviting applications for hiring of biometrics consultant" to assist in "proof of concept of biometric solutions for UIDAI project." This document is a startling statement of the state of ignorance of the UIDAI, while they had already decided that they would adopt biometric de-duplication and authentication. The consultant would have to "assess the biometric de-duplication accuracy that can be achieved in the Indian context."

The U.S. National Institute of Science and Technology (NIST) "has spent considerable efforts over the past 10-15 years in benchmarking the state-of-the-art extractor and matching technology for fingerprint, face and iris biometrics on the western population," the invitation document read. "While NIST documents the fact that the accuracy of biometric matching is extremely dependent on demographics and environmental conditions, there is a lack of a sound study that documents the accuracy achievable on Indian demographics (i.e., larger percentage of rural population) and in Indian environmental conditions (i.e., extremely hot and humid climates and facilities without air-conditioning). In fact, it went on, "we could not find any credible study assessing the achievable accuracy in any of the developing countries. UIDAI has performed some preliminary assessment of quality of fingerprint data from Indian rural demographics and environments and the results are encouraging. The "quality" assessment of fingerprint data is not sufficient to fully understand the achievable de-duplication accuracy." The consultant was given six months to lead the UIDAI from this state of ignorance to profound knowledge about biometrics. At that stage, the focus was on enrolment. The question of what would happen when people would have to be identified by their biometric markers was deferred to a later date (15).

The study was done between March and June 2010. On July 17, 2010, the *Economic Times* reported that "missing biometrics" was confronting the UID project. The millions of agriculture, construction, and manual workers would have their fingerprints worn down. Corneal scars, corneal blindness, cataract resulting from nutritional deficiencies and prolonged exposure to sunlight and ultraviolet rays were likely to jeopardize iris data. The Director General of the UIDAI reportedly admitted that they had no estimate of how many people this would affect – they expected it to be a "small number." "We are dealing with a large country and complex issues. We have to work within these limitations," he is reported to have said. We now know that despite the complex issues at hand, the authorities moved on regardless, to collecting biometrics while making claims of uniqueness.

The "UID enrolment proof-of-concept (PoC) report" was finally uploaded on the UIDAI website in February 2011, about five months after UID enrollment began roll out (16). In a report that is gloriously vague and hazy, there is one statement that puts a question mark on the whole exercise: "The goal of the PoC was to collect data representative of India and not necessarily to find difficult-to-use biometrics. Therefore, extremely remote rural areas, often with populations specialising in certain types of work (tea plantation workers, areca nut growers, etc.) were not chosen. This ensured that degradation of biometrics characteristic of such narrow groups was not over-represented in the sample data collected." The number of people in the sample studies to see if de-duplication worked was 40 000, and this did not include those who were not seen as representative of India! The report then maintains a deafening silence on the subject of what will be done for "biometric exceptions" – for people for whom neither fingerprints nor iris work.

## Risks Associated with Trailblazing: Failure, Legality, and Surveillance

The UIDAI would be hard put to term this a scientific study. There is no authorship, the complexity of the population is ironed out by excluding them from the sample, the evidence is sketchy, and the

conclusions are general. Two years later in his talk at the World Bank in April 2013 Mr. Nilekani was to say that "nobody has done this before, so we are going to find out soon whether it will work or not." Some days later, Mr. Nilekani openly declared in his speech at the Center for Global Development in Washington: "We came to the conclusion that if we take sufficient data, biometric data of an individual, then that person's biometric will be unique across a billion people. Now we have to find that out. We haven't done it yet. So we'll discover it as we go along" (4).

So, first, the conclusion; then they will wait to find out! Some observers of the project who have been saying that it is an experiment being conducted on the entire population, are justified. The consequences of failure have not been discussed, although, in a talk at the World Bank Mr. Nilekani said in response to a question about what he thought was the greatest downside risk to the UID: "To answer the question about what is the biggest risk," he said "in some sense, you run the risk of creating a single point of failure also" (5).

The UID project is proceeding without the cover of law. There is only the notification of January 2009 that says the UIDAI "owns" the database, but says nothing about how it may be used, or what will happen if it fails or if there is identity fraud, or if some outside agency gains access to the database. A Bill was introduced in Parliament in December 2010, after the project had been launched and data collection had begun. The Bill collapsed in December 2011 when the Parliamentary Standing Committee found it severely lacking, and found the Bill and the project needed to be sent back to the drawing board. There is still no sign of any protection that the law may offer. Neither is there any law to protect privacy.

The UIDAI and Mr. Nilekani have refused to address the probability of surveillance, convergence, tracking, profiling, tagging, and intrusions into privacy that is likely to result from the creation of the database of residents and the intended convergence. The link between technology, databases, governmental power, and corporate involvement in creating, maintaining, managing, and using databases has produced various scenarios of surveillance that we continue to ignore at our peril. PRISM is just one example of ambitions that can fuel a state. In the same period, the state has already set up agencies such as the Natgrid, NCTC, NTRO, CCTNS, and MAC, which exploits database integration that the UID makes possible. In April 2011, the government made rules under the IT Act 2000, by which it would be able to access any data held by any "body corporate." More recently, we have been hearing about the Central Monitoring System (CMS), speaking to a surveillance and control approach that will have the state snooping on us with no oversight, no prior permission, and no answerability at any time to anyone.

The companies engaged by the UIDAI to manage the database include L1 Identity Solutions and Accenture. The UIDAI, in response to a Right to Information (RTI) request, claimed that they had no means of knowing that these were foreign companies awarded contracts, given the process of their selection. Yet, a search on the Internet reveals the closeness between the L1 Identity Solutions and the CIA, and that after a 2011 transaction, L1 Solutions was partly owned by the French government. Meanwhile it was also well-known that Accenture was in a Smart Borders Project with the U.S. Department of Homeland Security. Data security, personal security, national security, and global surveillance are all drawn into a ring of concern, but remain unaddressed.

## What Is the UID?

UID is an acronym that stands for "unique identification." But the first thing we observe is that this is not an identity scheme; it is a system that leverages emerging technologies to help various governmental and commercial agencies identify and database persons. Second, UID is not a card, but a number. Some have mistaken the paper that is used to communicate the UID number to the resident to be an ID card: "(f)irst of all, this is not an ID card project. There is no card. There is a number. It's a virtual number on the cloud, and we don't give a physical card. We do send you a physical letter with your number, which you keep in your pocket, but the real value of this is the number on the cloud" (5). The identification is to be done by matching the number to biometrics that are collected and kept on a Central Identities Data Registry. The uniqueness of the number depends on the biometric system being failsafe; but biometrics is still at an experimental stage.

Third, while a driving licence, voter ID, and PAN card may be used as identity cards, the UID number is different. The UID is synonymous with the "Know Your Customer" (KYC) principle. The UID project proposed a partnership with Authorized User Agencies (AUA), which may include banks, mobile companies, LPG service providers, insurance companies, departments with the state and central governments, hospitals, and so on. When the AUAs decide to use the UID, they

will have to deploy fingerprint and iris scanners, which will be used to "authenticate," that is, verify if the person is who they say they are. This is a business model, where the UIDAI proposes to make its profits on authentication – the Strategy Overview document calculates that once the project reaches a "steady" state, it should be able to make Rs 288.15 crore (6).

> **The UIDAI has demanded that everyone, from the newborn to the oldest resident, be registered on its database.**

Fourth, the UID is supposed to be voluntary, but that was a deliberate untruth put out as part of the socialization exercise for the project, and because the UIDAI has no power to force anyone to enroll. After all, their legal status has always been highly suspect. In the first two years of enrollment, it was evident that there was little enthusiasm to get on to the database. It has never been clear what the point of the UID number was. The fact remains, it is still not clear. At the World Bank talk in April 2013, Mr. Nilekani said in answer to a question: "Obviously people don't know what benefits will come from this – even I don't know what benefits will come from this... But broadly, they know that this is some kind of a gateway to the future. There will be benefits. What these benefits are, they don't know" (5).

Declaring that the UID was mandatory changed things for people. How the idea of making the UID mandatory was sold to various government agencies is not widely known. We do know that the UIDAI had banked on the UID being made mandatory by different agencies even when it put together its *Strategy Overview* (13). The strategy was for the UIDAI to continue pretending that it was voluntary.

Five, the words "universal" and "ubiquitous" are used to describe the ambitions of the project. By getting everyone on the database, there is to be "universal" coverage. And by getting every possible agency to subscribe to the UID as a KYC, it is to be "ubiquitous." Mr. Nilekani, of course, explains that the UID is an "identity platform." It is "open architecture" on which many "apps" may be built. Unlike the driving licence, ration card, or voter ID, the UID has no direct purpose of its own. It is just an "ID verification system" and all manner of "apps" can be built on it. Direct Benefit Transfer is one such "app." And in explanation of what it will do, Mr. Nilekani states: "You can use the ID and create a credit history... or you could build an electronic health system." Since it is on a cloud, your health record will be portable and "you can take it with you wherever you go." Of course, this also "gives you complete traceability," of persons and their transactions. "Obviously," he admits, "it doesn't solve the problem of eligibility. You have to build some other systems for that" (4).

The casual disregard of the law, the authoritarian demands to hand over personal and intimate information, creating databases that put people at risk, and passing off half-truths and outright lies as facts are only among some of the very disturbing features of the UID.

## False Claims

The UID, it is claimed, will be an identity scheme that will remove the barriers that prevent the poor from accessing benefits and subsidies. Unfortunately for the UIDAI, this claim is already being severely eroded. What was projected as a project of inclusion is already turning into a threat of exclusion. The poor have been warned that if they do not enroll for a UID, if they do not have bank accounts, if those bank accounts are not embedded with the UID number, then they will become ineligible for the subsidies that they receive. That is the first obstacle that has been set up by the project.

Then, a person needs to produce a pre-existing document to be able to enroll; a voter ID, a PAN card, a driving licence, or one of the many cards that are listed. Those who do not have a document to establish their identity or those whose documents are not accepted by the enrolment agency – and this is invariably the poor and the less privileged – will need an "introducer" to help them get enrolled. The introducer, as was explained by the Demographic Data Standards Committee that reported to the UIDAI in December 2009, would be akin to a bank introducer – with one significant difference: while a bank introducer would be expected to know the person he or she is introducing, it is different process with UID enrollment (7).

The state government or other agency acting as Registrar would have to appoint an "approved introducer" to do the task. That is, introducers must be known to the Registrar, but do not need to know the persons they are introducing! The accuracy of the data is thus suspect. No wonder, then, that in January 2012 the Home Ministry protested that they could not accept UID data because it was insecure and unreliable (8).

A second stated ambition is that of reducing leakage in the system. Mr. Nilekani refers to himself as a plumber, plugging the leaks. No one would deny the pervasive corruption that has blighted many systems of distribution. The RTI, "transparency walls," public hearings, the use of technology to computerize, communicate, and monitor the movement of goods and grain, the opening of post office and bank accounts for payment of NREGA wages, the use of mobile phones to let people know when their rations limits are reached so that they may watch and collect their entitlements, the use of GPS to track the movement of vehicles carrying grain to the shops – these have already greatly improved systems.

The UIDAI, however, suggests that salvation lies elsewhere –in a centralized system of identification. Allegedly this would do away with duplicates and ghost beneficiaries. There is, of course, no evidence as to the extent of the leakage, and what the savings would therefore be. In fact, the first paper attempting to explain that the UID would reduce leakage was published by the National Institute of Public Finance and Policy (9). The paper is littered with assumptions for, as they admit, there isn't any data in some areas and, in others, the data is outdated. In addition, contrary to Mr. Nilekani's assertion at the talk in April 2013 that this was an "independent study," scholars at the NIPFP have admitted to "the group's research affiliations with the UIDAI should preferably have been made in the study itself." How many are aware of the One Time Passwords (OTP) which are to be used to "manual(ly) override" when the biometric identification fails (10)? When fingerprints or iris fail to recognize a person, for whatever reason, a request can be sent to the UIDAI to send a One Time Password to any mobile phone that is on hand.

The potential for "leakage" and identity fraud and corruption through the use of the OTP option, and the problem this poses for the "last mile" is undeniable, although it is not being acknowledged. No wonder everyone including the UIDAI is shrinking from taking on liability where there is a "false accept," or "false reject," or when identity fraud occurs. The risk thus rests heavily on the individual. For now, the hype that has surrounded the UID has been legitimized by past failures and corruption. However, the excitement surrounding the biometric technology is unjustified as it has not been derived by an intimate understanding of the poor and marginalized. The gap between the project's claims and how it is actually playing out in reality is huge. And how much the bureaucracy and the political establishment have understood is moot; they have spoken too little for us to tell. With the claims not quite holding up, one has to ponder what ambitions have driven the project?

In the early stages of the project, UID was postulated as the answer to the problems in the PDS and NREGA; but the credibility of these claims was severely challenged by researchers and activists. The focus was then shifted to "financial inclusion." UID was meant to fulfil the "Know Your Customer" (KYC) principle for opening bank accounts, more particularly what is generally acknowledged as "no-frills" accounts. The problem with this claim is that KYC in banking was brought in, in the context of money laundering, and terrorist funding. No-frills accounts have had no KYC requirement; the amounts are too small to matter. Now, with the UID, KYC has even been introduced for no-frills accounts. That so many people are unbanked has a great deal to do with banks not being interested in low value customers, not having branches where they are needed, and with the banking correspondent system not working. The banking system is totally unprepared for the changes that have occurred to date, and continue to occur. Rather, this has meant that some members of the population, panicked by the threat of exclusion, have rushed to be enrolled on the UIDAI.

## Toward a Global Identity System

At Nilekani's Washington meetings in April 2013 at the CGD (4) and the World Bank (11), discussions were drawn around what some might consider outrageous proposals. Addressing Mr. Nilekani, the chair of the meeting said: "I wonder what you think of the possibility of a global system, and whether or not you think by the year 2050 there could be a global system. Frankly, I think it would be a real influence in knocking down the nation state..." And then he asked, "Is this the thin edge of the wedge for the end of sovereignty?" The question recurred at the World Bank meeting (11) where Mr. Nilekani's answer was simple: "There is nothing technologically limiting for having the whole population of the world on the system... If you can do a billion, you can do 7 billion." The President of the World Bank then repeated that all projects brought to him, for Africa, and everywhere else, would now have to integrate the UID system, or else he would want to know why: "... can you have a single system that would work with everybody throughout the world?" And "what are the implications if you were to withdraw money... all ATMs may say, we don't want just your card and PIN number, we want your biometrics everywhere... you literally would know where somebody is every minute... or every time he did that transaction. Would you do one system?...

So, should we, say, if we start a system in Africa, we should coordinate with you, so that the Africans have different numbers than the Indian have." "Well," Mr. Nilekani responded, "this is a question of how much you want to centralize" [11].


## Acknowledgment

This article has been adapted from articles written by Usha Ramanathan between July 2nd and 6th, 2013 for *The Statesman*. The original content can be found at: http://www.thestatesman.net/news/3514-threat-of-exclusion-and-of-surveillance.html.



## Author Information

The author is an internationally recognized expert on law and poverty. She is a research fellow at the Centre for the Study of Developing Societies, and teaches environmental law, labor law, and consumer law at the Indian Law Institute, New Delhi, India. Email: urushar@gmail.com.


## References


[1] N. Nilekani, 2009, "Ideas for India's Future", TED, http://www.ted.com/talks/nandan_nilekani_s_ideas_for_india_s_future?language=en

[2] R. Dass, 2011, "Unique Identity Project in India: A Divine Dream or a Miscalculated Heroism?" Indian Institute of Management, Ahmedabad, India, http://indiagovernance.gov.in/files/UID.pdf.

[3] "National Citizen Database", Department of Electronics & Information Technology (DeitY), Ministry of Communications and IT, Government of India, http://deity.gov.in/content/national-citizen-database

[4] N. Nilekani, April 22, 2013, "Technology to Leapfrog Development: The Aadhaar Experience", The Eighth Annual Richard H. Sabot Lecture, Centre for Global Development, http://www.cgdev.org/sites/default/files/nandan-nilekani-sabot-lecture-transcript-technology-leapfrog-development.pdf

[5] G. Krishna, 2013, "Aadhaar: Supreme Court exposes complicity of political parties", MoneyLife http://www.moneylife.in/article/aadhaar-supreme-court-exposes-complicity-of-political-parties/34612.html

[6] U. Ramanathan, 2013, "Your Data, Going on Sale Soon", The Hindu, http://www.thehindu.com/opinion/op-ed/your-data-going-on-sale-soon/article4733606.ece

[7] Y. Bhavan and S. Marg, 2009, Demographic Data Standards and Verification procedure (DDSVP) Committee Report, New Delhi, Unique Identification Authority of India, Unique Identification Authority of India http://uidai.gov.in/UID_PDF/Committees/UID_DDSVP_Committee_Report_v1.0.pdf

[8] U. Ramanathan, 2013, "UID: An inclusion project that excludes the poor", The Alternative.In http://www.thealternative.in/society/uid-inclusion-project-that-excludes-the-poor/

[9] NIPFP, 2012, A cost-benefit analysis of Aadhaar, National Institute of Public Finance and Policy, http://planningcommission.nic.in/reports/genrep/rep_uid_cba_paper.pdf

[10] Planning Commission, 2012, "Authentication Overview", UIDAI, Government of India, http://uidai.gov.in/auth.html

[11] N. Nilekani, K. Basu, Jim Yong Kim, 2013, "The Science of Delivering Online IDs to a Billion People: The Aadhaar Experience", World Bank Live, http://live.worldbank.org/science-delivering-online-ids-billion-people-aadhaar-experience

[12] G. Krishna, 2013, "Are Indians being used as guinea pigs of biometric technology companies? -Part 14", http://www.moneylife.in/article/aadhar-indians-used-as-guinea-pigs/35520.html

[13] Planning Commission, Govt. of India, 2010, "Strategy Overview: Creating a Unique Identity Number for Every Resident in India", Unique Identification Authority of India, p. 13, http://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overveiw-001.pdf

[14] UIDAI Committee on Biometrics, 2009, "Biometrics Design Standards for UID Applications, Unique Identification Authority of India Planning Commission", http://uidai.gov.in/UID_PDF/Committees/Biometrics_Standards_Committee_report.pdf

[15] U. Ramanathan, 2010, "A Unique Identity Bill", Economic and Political Weekly, Vol. XLV, No 30, p.13, http://ielrc.org/Content/a1003.pdf

[16] UIDAI, 2012, "References", Unique Identification Authority of India Planning Commission, http://uidai.gov.in/publication-and-reports.html


TS

# BOOK REVIEW *(continued from page 5)*

the Library of Congress archives Twitter feeds, [3] and commercial data brokers mine publicly-available data items to paint a disturbingly-accurate digital portrait of us [4]. Eggers' story reminds us that vigilance and societal self-examination are necessary for a moral society. Once the world has been digitally quantified, it can be made visible. Once it has been made visible, it can be controlled.


***Scott D. Eldridge** received his B.S.C.I.S. degree from The Ohio State University, College of Engineering and his B.F.A. degree in photojournalism from the Corcoran College of Art + Design. He has worked as a test engineer and project manager in aerospace and technology companies for over 16 years, and he is currently pursuing his M.A. degree in the Communication, Culture, and Technology program at Georgetown University. Email: scott.d.eldridge@gmail.com.*


## References


[1] H.F. Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford, CA: Stanford Law Books, 2010.

[2] S.R. Peppet, "Unraveling privacy: The personal prospectus and the threat of a full-disclosure future," Northwest. Univ. Sch. Law Rev., vol. 105, no. 3, pp. 1153–1203, 2011.

[3] E. Allen, "Update on the Twitter Archive at the Library of Congress | Library of Congress Blog," Library of Congress Blog, Jan. 4, 2013. (Online). Available: http://blogs.loc.gov/loc/2013/01/update-on-the-twitter-archive-at-the-library-of-congress/. (Accessed: 03-May-2014).

[4] M. Hicken, "Data brokers sell lists of rape victims, AIDS patients, privacy group finds," CNNMoney, Dec. 19, 2013. (Online). Available: http://money.cnn.com/2013/12/18/pf/data-broker-lists/index.html. (Accessed: 03-May-2014).


TS