Health and Technology (2017) 7:265–324
https://doi.org/10.1007/s12553-017-0211-5

EDITORIAL

# Interrogating “privacy” in a world brimming with high political entanglements, surveillance, interdependence & interconnections

Robert Mathews [1]

Received: 3 November 2017 / Accepted: 16 November 2017 / Published online: 4 December 2017

## 1 Introduction & orientation

More than 4 decades ago, Sociologist Daniel Bell in *“The Coming of Post-industrial Society”* [1] attempted to draw people’s attention to the impending transit of the United States’ from a smoke-stack, assembly line-industrial economy to something different – quite different, a knowledge intensive creative economy, where entirely different skill-sets than those the ‘educational factories’ were dispensing to “future workforces” would be needed. Fundamentally, Information and Communications Technology (ICT) tool-chest dominated ‘knowledge creation’ economies were going to present different societal challenges.

24 years later, at the dawn of a new millennium, Sir Leon Brittan, then Vice-President of the European Commission, speaking at the EU-Japan Cooperation Week in Tokyo lamented that the European Community was *“…managing a difficult transition to becoming post-industrial societies with aging populations”* [2]. To be sure, in his speech, Sir Leon was surely not ruling out mal-adjustment among other nations outside the European Community. From germane observations, 20 more years beyond Sir Leon’s speech that day, all are still wrestling poorly with key transitional pathways into post-industrial societies.

History will judge humanity as not having been well equipped to deal with the self-created problems of the industrial world [3]. Could we blindly expect humankind to be anticipatory, and be prepared to deal with challenges we summon and make plain in a post-smokestack world? Beyond the historicity of the Industrial Revolution’s burning waters itself, is that ever unfamiliar ‘transition phase’ from one world into the next, where aging and inadaptive populations, failing educational systems and new skill-set demands, new thought directions, failure to systemically understand changes occurring at societal components,[1] and associated interfaces[2] have only exacerbated running issues related to Personal Privacy and Security.

Privacy is a deeply misunderstood concept[3]; one that is experienced, protected, defended, adjudicated, and enforced in highly inconsistent ways across legislative, judicial, cultural, linguistic, economic, social, racial, ethnic and inter-national boundaries. Likewise, and to make matters worse, generally, parties fail to understand and to represent correctly, the linkage/relationship between privacy and security in models spoken of, or in those models that are employed in society. This aforementioned lack of understanding and representation is at least in significant parts, connectable to states of global transitions to informational societies, and attributable to our inability to transit, and acclimatize to a post-industrial world. Collectively, given the aforementioned paradoxes,[4] where, pervading failures to understand the meaning of

This article is part of the Topical Collection on *Privacy and Security of Medical Information*

The views expressed in this editorial chapter are solely that of the author, and do not reflect the official policy or position of the University of Hawai’i, the Office of Scientific Inquiry & Applications (OSIA), or the United States Government

✉ Robert Mathews
mathews@hawaii.edu

[1] Distinguished Senior Research Scholar, National Security Affairs & U.S. Industrial Preparedness, Office of Scientific Inquiry & Applications (OSIA), University of Hawai’i, Honolulu & Hilo, HI, USA

[1] Sample discussion of this can be seen in “2.2 Privacy Knowledge Boundary and Its Implications”

[2] Sample discussion of this can be seen in “6.1 Road To ‘High Trials’ In Privacy & Security”

[3] See discussion under “2.1 Need For A *Lingua Franca* for Privacy and 2.2 Privacy Knowledge Boundary and Its Implications”

[4] We want and need interconnected Privacy and Security solutions immediately, but our inability to understand Privacy and Security meanings to the breadth and depth required relegates us to a state of incapacitance in relation to the formulation of solutions

Privacy, and failures to properly orient Privacy actions and reactions to necessary security concepts and constructs, combined with shortfalls in each of our 'very personal configuration,'[5] make for exceedingly potent barriers to clarified and universal expressions of Privacy as a desired and cherished value in societies. Our 'personal configuration'[6] tends at least be a significant barrier to organizing and building Privacy relations with others in the world. All shortfalls in our 'personal cultivation' therefore, lead to a strengthening and amplification of the difficulty we commonly have toward affirming and promoting Privacy and Security ideals in our individual living environments.

Former U.S. Supreme Court Associate Justice and social justice champion Louis D. Brandeis left behind some resplendent perspectives for contemporaries, and to aid future Americans and people in the world over, some fertile thoughts and stable directions toward societal regularization and commeasurement, and essential themes and concerns to one's personal cultivation to chance a more ideal "personal configuration" for all. One such thought of Brandeis was to urge U.S. States and their respective populations to address critical constitutional, political, and societal maladies through entrepreneurial experimentation and political risk management. Brandeis represented this thought through a dissent he had formed, hoping that by such experimentation, accompanying experiences and learning would expose all - to more qualities befitted to maintaining a stronger, more idyllic republic, and would collectively leave behind a stronger people. Nonetheless, in the same breath, he acknowledged how difficult a task such 'experimentation' would likely be, without an appropriate 'personal configuration' and the need 'to be measured' in the course of experimentation itself. Delivering his dissent, Brandeis emphasized, *"[t]o stay experimentation within the law in things social and economic is a grave responsibility…"* and added, *"[i]n the exercise of this power, we should be ever on guard lest we erect our prejudices into legal principles. If we would guide by the light of reason, we must let our minds be bold"* [4]. Apart from other things, society is forced to have to look to Brandeis again, if we are to follow his counsel and place into practice - those means to defend against the injection of "our prejudices into legal principles" capable of easing the disappearance of fundamental human rights everywhere. In, and for similar endeavors, Brandeis directed that "[t]he first essential of *wise and just action* is knowledge" [5]. Therefore, following a beckoning from Brandeis, and to infuse several Privacy fundamentals as an introduction to the totality of the information from our valued contributors to this Special Issue on Privacy and Security, this Editorial Chapter shall aim to present a more wholistic and foundational understanding of Privacy attributes - universally desirable among the participants in the "*Fourth Industrial Revolution"* [6].

This writing will examine "un-fused" aspects of Privacy; composings of human evolution, nature of our 'civilizing;' personal constitutions and degrees to which we think ourselves to be civilized, our behaviors, organizations, national and cultural identities, personal preparation and coping abilities in the face of rapidly evolving technologies, shifts in labor forces, systems of governance and governments. Consequentially, this collection of thoughts will not be a preoccupation with listing all the latest information system' compromises/penetrations, or how many of those compromises/penetrations occurred in this past year, rather, it will be a representation of certain Privacy and Security aspects that are not often discussed. For example, by taking account of the many Socio-Economic-Political happenings in India and the country's rich history, we begin to understand the Privacy and Security imperilment the nation and her people now face, despite the 'global waypost' of a Privacy ruling rendered by the Supreme Court of India [7]. Also, a brief background examination to Privacy related developments in Rwanda, in a post genocide time is included. Lastly, a significant portion of this writing will be devoted to an examination of Privacy/Security values and the human dimension. Examinations will attempt to cover broadly, some of the Digital Century's "Human Resource" (HR) challenges in terms of "organizing" to protect Personal Privacy, and "organizing" to ensure the Security of sensitive information. Contextually, the author will aim to highlight specific factors deemed to be detrimental to the composition and retention of effective, productive, and efficient 'knowledge teams.' The examination will also inspect how interconnection and interdependence of "information age" HR challenges are expected to affect institutional abilities to leverage capacities judiciously, capabilities, and resources gravely to protect and preserve Personal Privacy and Information Security for the future.

## 2 Interrogating "privacy"

Does Privacy know, who, or what, Privacy is? Since a conversation with "Privacy" per se is impossible, the next most logical step must be one aimed to catechize ourselves on the subject of Privacy. We must examine the very nature of our frangible understanding of Privacy, the texture and temperament too. Let us begin with Annabelle Lever's sentiment relating to the general difficulty and the inability to gain the pulse of Privacy. Lever says, *"the challenge of providing a philosophically satisfactory account of privacy—assuming that such an account is possible—is to find some common starting point from which we can articulate and evaluate*

[5] Our individual breeding/upbringing, and the extent to which each of us have forthrightly endeavored to shape (groom) ourselves to become civilized, and is therefore prepared and organized (i.e., configured) to interact (act upon and react to) routine and non-routine situations involving declared concepts and/or conventions related to universal human rights

[6] *Ibid*

*competing intuitions and perspectives on privacy—on what it is, on how it differs from related concepts such as liberty, on whether it is valuable, and on whether it deserves legal protection as of right. Otherwise, we are left with the trading of intuitions, which dominates much of the philosophical literature on privacy…"* [8].

This author could certainly agree with at least one aspect of Lever's writings, which is, we have mainly been trading intuitions this far, and we shall continue to do the same for a lot longer, unless some strong intellectual horsepower is applied to the problem. There are solid pathways by which, productive and clarifying discussions related to Privacy can be had. Why then, are such pathways not being utilized? It is because we are too busy clouding those pathways with casuistry and prevarications, only to lead to the production of subjective and whimsical reference points for the sake of penning scripts, which might prove to be 'syntactically correct, yet semantically meaningless.'[7] The reader should be reminded of Lever's statement once more, wherein she highlights the need to evaluate *competing intuitions* and *perspectives on privacy;* and emphasizes in a way, that differences between the concepts of *Privacy* and *Liberty* (for example) will need reconciliation, for advancement to surface.

For the purposes of this Privacy interrogatory, it would be appropriate to seek and find a directional beacon to orient Privacy and Security considerations and discussions properly. The one universal substrate onto which 'Privacy values' could be properly docked, is the Universal Declaration of Human Rights (UDHR),[8] which is now widely agreed to be the foundation of international human rights law. If the UDHR is to be the foundational basis for all considerations related to Privacy (and it is), then, as an example, all need to ensure that *"esteem for human life"*[9] does not become a value target, or a negotiable goal that could ever be mutilated by the presence of clashing or *competing intuitions,* or *perspectives* (as offered by Lever) – driven for instance by, cultural or religious differences within populations.[10] Lever correctly observes that the World of Privacy has been clouded with competing intuitions and perspectives of people. Continuing, extending '*respect for life'* is a value that is universally acknowledged and accepted as being durable and unchangeable. Yet, in many parts of the world, and as the reader will become acquainted, people's lives are forcibly taken from them. When people are not willing to respect life, how then can such people recognize Privacy as a desired human value, or as an integral part of Human Rights universally?

Approaches to the framing of modern day Human Rights[11] has been with us for Centuries,[12] and essentially began with man's desire to be emancipated from the savage beast that he is, and to foundationally organize practicable, illuminated, vibrant and nonbelligerent societies – taking into account, moral and legal thoughts, also considering concurrently, vast knowledge from other branches of Philosophy such as Logic, Ethics, Epistemology etc., Therefore, it is proposed that nations and their respective populations that chose to accede to the principles made clear in the UDHR would not have done so lightly, and must have been prepared to abide by said principles. Privacy as a privilege under the UDHR was never intentioned to receive a lesser consideration or treatment in view of other principles. To that point, Lever has sought considerations from her readers to take note of the challenge associated with affording formalized legal protection to Privacy.

Quite surprisingly, on 24 August 2017, in the world of Privacy, the North, and South Poles swapped places, when the Supreme Court of India declared that Privacy was a fundamental right for nearly 1.4 billion people of the world. To that time and space, no country and certainly no court in the world, had declared ever so plainly and importantly that salient fact, so fundamentally rooted in the UDHR. Still, what will the Indian Supreme Court ruling mean to all Indian citizens? Many fundamental human rights still elude Indians, and the ways in which ordinary citizens are able to seek redresses for wrongs committed, and those other wrongs to be prevented, are in an entirely primitive or corrupt state; moreover, both institutions and pathways necessary to address wrongs committed and to the prevention of others, could well be considered to not exist. It can perhaps be said, and safely, that, India will be least prepared to advantage all Indians by way of the landmark legal Privacy ruling, primarily due to near overwhelming social and politiical challenges.[13]

Elsewhere in the world, and purely in terms of identifying our very personal 'Privacy' meanings and its valuable tinctures, each of us are bound to be confounded by terms such as *'liberty,' and 'freedom,'* in relation to the Privacy, which continues to be part of the *"semantics"* battle, and *'…the trading of intuitions,'* which is at the very least, an activity that trades in *"pure passion"* [9]. Fmr. Dean of the Yale Law School, Robert C. Post has summarized the involvedness surrounding

[7] The author directs the curious reader to a discussion of Lewis Carroll's work: "The Comprehension of Nonsense – Carroll's "Jabberwocky" and Neologism" In: Dolitsky, Mariene; "Under the Tumtum Tree: From Nonsense to Sense, A Study in Nonautomatic Comprehension," In: "Pragmatics & Beyond: An Interdisciplinary Series of Language Studies," [Hubert Cuyckens, Herman Parret and Jef Verschueren, Eds.], John Benjamins Publishing Company, Amsterdam, Netherlands, 1984

[8] "The Universal Declaration of Human Rights," adopted by the UN General Assembly, 10 December 1948 https://www.un.org/en/universal-declaration-human-rights/

[9] This topic will be discussed further under the section "5. The Case of Privacy in India"

[10] *Ibid*

[11] Which has Included discussions on the matter of Privacy itself, and aspects such as encroachment upon, or compromise of, Privacy, lawful and unlawful actions etc.

[12] This is a subject that will clearly be discussed more in section "5. The Case of Privacy in India"

[13] Some of these challenges will be discussed within section "5. The Case of Privacy in India"

Privacy in the following way. Post said, *"[p]rivacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I some-times despair whether it can be usefully addressed at all"* [10]. In writing as regards "*competing and contradictory dimensions* on Privacy, to what does Post reference? Could Post be speaking of Lever's [11] *"competing intuitions"* and the many *"perspectives on privacy"*? In the here and now, you must be the judge. However, Privacy related societal progress appropriate for the Digital Century could only emerge from resolutions to, and reconciliations in, confoundings surfaced within the many perspectives on Privacy.

As an example, a basic confusion, durable in contemporary discussions related to privacy involves the Late Associate Justice of the United States Supreme Court Louis D. Brandeis and his scholarship on Privacy with Samuel D. Warren. For many Privacy practitioners and scholars the world over, the "go to" tree-root of Privacy seem to be is their 1890 article that appeared in the Harvard Law Review, titled: *"The Right To Privacy"* [12]. No question that the world owes a great debt of gratitude to Warren and Brandeis for their very important legal scholarship on Privacy however incomplete or evasive (as posed by Richardson) [13] Warren, and Brandeis were in their scholarship. Also, there can be no question, that Louis D. Brandeis was a social justice champion. Brandeis's legal writings and his role separately in the American Judiciary as an Associate Justice of the United States Supreme Court further advanced key Privacy ruminations around the world. However, there exists no karmic dictate, which declared it necessary for all Privacy epistles to begin, or end, with hurried and mechanical references to Warren and Brandeis. The subjects of Privacy, and indeed Security of personal information and of-self, have been important topics for discussion since before Warren and Brandeis. There need be little argument that the title of Warren and Brandeis's scholarship has at the very least, assured their body of work a safe passage into the after-life [14].

Another point of confusion involves the origin of certain core ideas in relation to Privacy. To clear-up these elements of confusion, consider for a moment that Warren and Brandeis had noted in their writing that *"[t]he press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery"* [15]. They then published their work in December of 1890. Meanwhile, the Anglo-American editor and newsman E. L. Godkin penned a collection of thoughts, and he too, published it widely in the month of July - also in 1890. Godkin wrote: *"The chief enemy of privacy in modern life is that interest in other people and their affairs known as curiosity, which in the days before newspapers created personal gossip."* In addition, Godkin said, *"[c]uriosity, in its larger and nobler aspect, lies at the root of Western… civilization. In its smaller, pettier, and more ignoble shape, it became the passion of the Paul Pry and the scandal-monger* [16]. Perhaps the reader is able to distinguish a trace of similarity in thought - from both sets of authors.

In that which amounts to be no more than a diminished reference in their writing (in footnote number 48), Warren and Brandeis managed to speed by Godkin's thoughts, largely as something that was published earlier, in 1890. However, notably missing in any of their joint article related to Privacy is the foresighted, down-right oracular text that Godkin had written and published in 1880; a decade earlier than Warren and Brandeis's writings that began to popularize the notion of the right "to be let alone." In his writings of 1880, Godkin said, *"…we must admit that nothing is better worthy of legal protection than private life, or, in other words, the right of every man to keep his affairs to himself, and to decide for himself to what extent they shall be the subject of public observation and discussion"* [17]. At least on surface, these ideas appeal similarly, in all manners of form.

In addition, while Warren and Brandeis made note in their article that Jurist Thomas Cooley originated the thought: "to be let alone" in 1888, copious writings on Privacy since, point to Warren and Brandeis as originators. Cooley, In *"A Treatise on The Law of Torts,"* [18] had asserted that "to be let alone" can be said as, a right of "complete immunity." The following statement by Cooley is far more significant in spirit, and in moral weight, than most things that were written at the time, and is perhaps not well surfaced or discussed at all. With respect to Privacy, Cooley said that, *"[t]he corresponding duty is, not to inflict an injury, and not, within such proximity as might render it successful, to attempt the infliction of an injury"* [19]. These points are intended to convey certain simple yet non-trivial facts that weighty Privacy discussions did occur prior to Warren and Brandeis's writings in the Harvard Law Review, and two, we must investigate what it is that we truly understand of Privacy in relation to longstanding discussions. These are not minor points in relation to this Journal' Special Issue.

### 2.1 Need for a *Lingua Franca*[14] for privacy

Privacy desperately needs a common language, and a universal frame of reference, but it lacks for one. The Universal Declaration of Human Rights (UDHR) is perhaps the most appropriate axis of rotation to unify the many, if not most, Privacy and Security elements and corresponding bases. Despite many signatories to the UDHR, and the number

[14] *Lingua Franca* \ Noun \ 1. A language that is adopted as a common language between speakers whose native languages are different. 1.1 historical \ mass noun \ A mixture of Italian with French, Greek, Arabic, and Spanish, formerly used in the eastern Mediterranean. Oxford [English] Living Dictionaries https://en.oxforddictionaries.com/definition/lingua_franca

of nations that have ratified the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR), tangibly expressed practices of respect for Privacy, in relation to the UDHR has still to be seen universally. In many areas of the world, including the most developed - there are strong desires to subjugate fundamental human rights in the name of security. Widespread misunderstanding in the meaning of Privacy, and of the scope on being able to apply Privacy principles in society, aid in the perpetuation of societal and situational conflicts and consternations.

Moving into this section, the most important leading question to be asked is, if people around the world are to protect Privacy and they do not have a well-articulated, universally logical, and comprehensible framework for Privacy decision-making and protection, how will it be possible to extend Privacy protections across multiple borders, languages, cultures belief-systems etc., especially when, questions or concerns related to "Security" are not (or cannot be) reconciled or resolved. Privacy meanings, orientations, societal valuation, laws, situational evaluations, actions, etc., must all have some universal connection, meaning, emphasis, and alignment. As it is said in the United States military, *one must train, as one is likely to fight.* If there is a mismatch between acquired training on how to protect, and the real conditions encountered in the ecosystem where the protective training is to work, then there is likely to be a failure in protective measures deployed. A pair of comparable instances, highlighting process and procedure errors is disclosed below to demonstrate the weight of aforesaid needs, and the fragility that likely surrounds Privacy and Security protections.

**Dateline: 5 December 2001.** For the United States, the conflict in Afghanistan has begun. *"Texas 12,"* a U.S. Special Operations Force (SOF) team consisting of CIA operatives, U.S. Army, and a USAF Combat Air Controller is inching toward Kandahar from northern Afghanistan.[15] Grouped to *"Texas 12"* is another team, similarly composed - designated *"Texas 17,"* also working its way toward Kandahar from the Southeast, near Pakistan. This day, the task for both teams is to keep Hamid Karzai (the man who would later become President of Afghanistan) and those others associated with him - out of harm's way, and allow him to arrive in Kandahar, and to negotiate the Taliban's surrender. *"Texas 12's"* Air Controller had been on continuous duty for a long while. Owing to this, he was relieved by an Enlisted Terminal Attack Controller (ETAC), who was unfamiliar with the equipment being used. It was then, that *"Texas 12"* was drawn into a close terrain firefight with the Taliban, at which time, the ETAC summoned USAF Close Air Support (CAS). During the firefight, the ETAC decides to change the batteries in the local GPS unit as a precautionary measure to prevent 'loss of GPS track' for the Close Air Support (CAS), not realizing that after any battery change, the GPS unit would reboot/reset, and when it did, it would start to transmit the location of the home-team, *"Texas 12"* (default setting), as opposed to the enemy's coordinates as necessary. An orbiting USAF B-52H '*Stratofortress*' answers the call for CAS, and releases a GBU-31s, a 2000 Lb. (908 Kg.) inertial navigation and GPS guided Joint Direct-Attack Munition (JDAM) toward the received coordinates. The result? Three U.S. Special Forces soldiers and 23 Northern Alliance fighters are killed. Luckily, Karzai is only knocked unconscious in the melee' The 'smart-bomb' impacted - a mere ~110 Yards (roughly 100 Meters or 330 Feet) from those who were killed, when the 'margin of safety' distance for friendly forces in the case of such a munition use was, ~1334 Yards (~1219.81 Meters or 4000 Feet).[16] If the people were better trained on processes and the technology, these "friendly-force" deaths could have possibly been avoided. That is a sentiment that is heard repeatedly, in relation to fratricide events. It has been identified that, carelessness; disorientation; confusion; poor leadership; inadequate training and experience on such things as procedures and communications; language barriers; lack of appreciation of technology, technology deployment area, and action ecosystems are some of the problem facets behind fratricide [20]. *Nevertheless, does training fix such problems in the modern world?* Recognizing that this is not a writing to present an analysis or a critique of U.S. military operations, that which is about to be presented is being done so, considering a forthcoming concentration upon the quality of people employed in the enterprise, and particularly in connection to "mission centeredness." Mission success in Close Quarters Combat (CQC) or Close Quarters Battle (CQB) requires continuous flow of information/communication, and situational clarity. Operationally, the need for continuous flow of information/communication and clarity is not a request; it is a requirement. Surprise, speed, and lethality - applied correctly upon the desired target are at the heart of CQC/CQB. A CQC/CQB "win" is necessarily a by-product of good people, strong skill-sets, resources, capacities, capabilities, and highly integrated teamwork. A "*Lingua Franca*"[17] is a foundational ingredient necessary to manifest precision and clarity in the continuous flow of information/communication between members of a highly integrated team. Regardless of situational specificity, operationally, "*Lingua Franca*"[18] in the command, control, and communications chain critically enables the ability for qualified interpretation, assessment of situationals, validation, verification, tasking, monitoring, and assessment. Naturally, "*Lingua Franca*"[19] is not

[15] Included details have been drawn entirely from *Unclassified* professional sources by the author

[16] *Ibid*

[17] See footnote # 14 (The 'language' inferred here with respect to battlefield activities is one of consistency; consistency in professional commitment, proper leveraging of benefits from training and experience, the wholistic and competent employment of natural and acquired skills, precise task orientation in relation to situational awareness, fidelity in action and reaction, task execution quality etc., to meet team/mission objectives.)

[18] *Ibid*

[19] *Ibid*

a substitution for other valid components being present, and/or meeting the appropriate standards, as in the need for the presence of highly capable people. "Fidelity" in actions taken to Protect Privacy, and the Security of Information requires no less preparation and readiness than the attention to detail, which is exercised in a battlefield to win against the enemy.

Phillip Barks (Lt. Col. USAF) wrote in a 2009 research report that, as in the aforementioned event near Kandahar, military history has continuously shown the demand for Close Air Support (CAS) being crucial in every major U.S. military action since World War II, in Korea, Vietnam, Kuwait, Afghanistan, and Iraq, and that each operation has resulted in some form of air-to-ground friendly fire incident [21]. Barks also noted that *"[f]rom the first day of training, individuals involved in the planning and execution of CAS have it implanted in their psyche that fratricide is tantamount to mission failure"* [22]. If, in a national military situation, such a strong imprint is made on trainees, where then – by it, a united recognition exists that fratricide was "not to stand," and in addition, they are told that fratricide would result in "mission failures," why does fratricide still happen, and happen so predictably? What can we expect in the Privacy and Security world in this respect? What can be learned? One thing is certain, enterprises must not permit carelessness; disorientation; confusion; poor leadership; inadequate training and experience on such things as procedures and communications; language barriers; lack of appreciation of technology and technology deployment in theater/combat area and combat actions in integrated information ecosystems [23]. These entrenched contributors to "mission-death" must be driven-out from the enterprise (See Fig. 1), in this case, for such purposes as the protection of Personal Privacy and Security. This primarily means organizations, teams and objectives must be constituted appropriately to quash "human errors"; [24] people involved in critical activities must be of a much higher professional caliber, pronounced personal quality, and fully capable of higher productivity. The low-quality of workforces has long been of interest to employers, at least in two respects: 1) in terms of employer demands and employee qualifications and competence mismatch in the labor force, and 2) quality of employee outputs/ productivity in the enterprise [25].

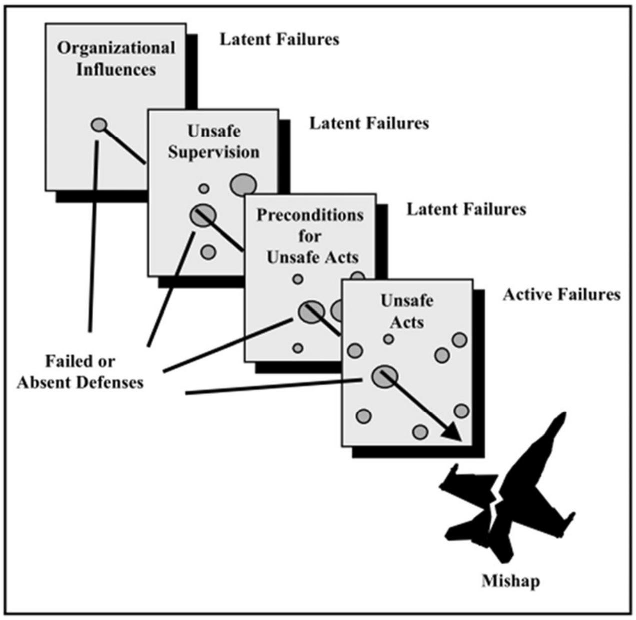


**Fig. 1** The "Swiss Cheese" Model of Human Error Causation. ("Human Error," James Reason, 1990) In: The Human Factors Analysis and Classification System – HFACS. Shappell & Wiegmann (2000)

As an adjacent note, the world of warfighting has advanced significantly since World War - I. General Alexandre Percin (France) wrote in his book "*Le Massacre de notre Infanterie,*" that, two artillery shells out of every ten (20%) in World War - I that fell on the soldiers in trenches were from friendly artillery [26]. During World War - I especially, Percin did not have command over a standardized French military, and did not have the ability to manage the quality of forces to improve them, for *Operational-Tempo* among other things at the time did not permit it. Today, despite the many advances that have been brought to the battlefield, including multiple ways to improve the quality of fighting forces, fratricide, or "friendly-fire" as it is called, continues to claim lives. Since 5 December 2001 near Kandahar, fratricide continues to occur. On 17 April 2002, it happened again near Kandahar; then again on 23 March 2003; 28 March 2003; 22 April 2004; 6 April 2006; 26 August 2006 and 5 December 2006, and on, and on, and on. Focus upon people, upon what they do, and how they do, must be a pre-eminent concern at all times. At least in one specific incident involving the death of a high-profile soldier named Pat Tillman on 22 April 2004, the U.S. Army attempted to cover-up the details of that fratricide [27].

From an *Interoperability*[20] point of view, every actor, organization, and resource in the chain-of-command and the chain-of-action - should be highly coordinated to be mission centered; being confused or disoriented are not acceptable conditions or outcomes in any action-chain. One wrong move and lives are lost, as it has been made clear, and repeatedly. Operationally, people, processes, and technology trains require tight integration at every level. Imagine a Medical Operating Theatre where everyone except the surgeon is focused on something other than the primary task, which is the surgery; what is bound to be the outcome? The ability to offer protection to Privacy & Security requires such tight

[20] ***Interoperability*** is rightly defined as that capability by which, all operating elements of interdependent and interconnected systems are able to synchronously operate and perform optimally to achieve objectives, or mission success (in this case, it is Personal Privacy and Security of Information). Synchronous operations here infers to an operational requirement for all components/subsystems of interconnected and interdependent systems, to be properly oriented, skillfully aligned, and to be reliably available — across any and all geographic and organizational boundaries, and professional disciplines to achieve mission objectives

integration. In the Armed Forces, sequential and continuous training, and employing the concept of "training as they fight" minimizes the risk of individuals in a team becoming lazy, confused or disoriented, increases the ability of identifying poor processes and procedures early, and in familiarizing personnel to precision in communication, action demands and personnel focus to tasks – to avoid deadly mistakes. To be able to focus 'combat power' upon the enemy requires 'applying' among other qualities, good battlefield judgement (which comes from levels of training) and high degrees of operational competence; Privacy and Security demands no less from operators at any involved level. Everyone has to be aware of, and be certain of, the actions that are being taken, or those that will be taken, in matters related to Privacy protection.

The second comparable instance of 'wrong targeting' is as follows.

> "Using a standard military map, a forward observer calls in grid coordinates for a fire mission. The field artillery battery receives the mission and the fire control crews initialize their state-of-the-art ballistic computer in accordance with the operations order (OPORD). The rounds impact[ed] 200 meters short of the target." – Major Richard J. Manning (USAR) [28]

Major Manning wrote in the Journal of Military Intelligence, that, "the problem was human error." Manning added that, "the misuse of datums and grids is a problem in our [U.S.] modern military. Many soldiers and leaders do not understand and are often mystified about how to employ datums' and grids properly." In the situation above, coordinates generated from a current map with the North American Datum 1927 (NAD-27) was used, all the while, the fire control battery was using the military standard World Geodetic System 1984 (WGS-84) datum in their computers. To clarify, Manning went on to say that, "datums are like different languages—without a translator they are incompatible with one another, in this case providing a different physical view of the earth for what appears to be identical grid coordinates" [29].

When engaged in the protection of Personal Privacy, or ensuring the correct employment of Security measures, none can afford to be speaking different languages. At present, we simply are. The proper use of technology tools, techniques, processes etc., becomes the responsibility of human beings. The language in this case, and more fundamentally, any semantic inconsistencies with regard to the language of choice employed in communications, is the responsibility of the adults on the scene. In the situation described above, the people-processes-technology train related errors have struck again. Such errors cause core missions to become compromised, and casualties and/or collateral damage to pile-up. Each component in the people-processes-technology train should be afforded deep attention always.

Considering the 'people component' only, we would all be well served to acknowledge, and to be reminded that in the absence of a universal reference, Privacy, and Security assurance, endurance, and reliability in large part will be attributable to, and be influenced by, aspects of human behavior and various societal norms; introducing great inconsistencies, and far less assuredness. At least within a military, there are standards of reference, methods of assessment, and means of operations etc., to ensure safety and the security of personnel, and overall operational quality and consistency. Even when there is the high-probability for less organizational, process, and procedural errors more specifically, there are likelihoods of human errors, which, a national military, or the likes of Medicine as an area/field cannot afford to have present within its personnel ranks.

Quite unfortunately, the misconstructions and categorical mix-ups involving Privacy and Security that can occur among people are not minor issues. The lack of axiomatic comprehension of Privacy and Security themes, topics, problems, and the absence of solid and reliable wholistic analytical systemic frameworks [30] and the absence of solidity and reliability in laws and judiciaries protecting against encroachments [31] etc., makes the upholding of Privacy and Security value in societies very difficult, if not downright impossible.

To ensure Privacy protections, and to strike a balance between use of Privacy, and Security instruments in society, there are no scientific, concretized means – even those means that are at least comparable, to be relied upon to establish such a balance. The absence of more universally judicable and expressible Privacy and Security measures and/or equivalents are material barriers to properly assuring privacy and security in every instance, and is of great societal significance. Said in another way, *"[i]n centrally considering Privacy [or Security], and how one might safeguard against encroachments upon it, or its loss, one must well appreciate that no entity can be protected adequately if the value of that which is to be protected, and/or the consequences related to its loss are not well understood"* [32].

Imagine that there is an intention to insure an item of some value. At a minimum, an insurance company must be provided with a reliable description of the item, an assured assessment of the item's inherent value, and all protective precautions that will be in force to keep the item safe, before any insurance company will consider undertaking the issuance of an insurance instrument of indemnity. After more than 50 solid years of contemporary discussions related to Privacy and its relationship to Security, why has it not been possible to establish a similar framework of obligations for Privacy and Security, as it has been the case in insurance to indemnify properly? The answer is quite simple. Fields of scientific study and practice have not advanced sufficiently in the multiple areas of concern.

However, Science – in the matter of needing to assure Privacy and Security, must advance, and appropriately, if the "*Fourth Industrial Revolution*" [33] and the Digital Century, both of which we are now immersed in - is to be of service to humanity. We must leverage scientific principles to humanity's advantage, to assert conditions of Personal Privacy. However, science cannot be leveraged to advantage Privacy *"… at the expense of 'wisdom-in-debit'; true wisdom empowers us with the ability to observe 'a matter,' to be reasoned to it, and from it, in all manner, to be prudent, discerning, relational, expressionally lucid, and analytically incisive of the whole, and not just any single part, or a collection of select parts"* [34]. We can neither "observe 'any matter'," such as Privacy or Security, nor adequately "be reasoned to it" as stated above, if we are not equipped with the proper knowledge, tools, and the correct subject matter orientation most of all.

In his seminal book on the subject, the Late Alan Westin[21] spoke of this eminently. Upon the motivating of the Special Committee on Science and Law of the Association of the Bar of the City of New York, and with financial support from the Carnegie Corporation, in 1967, the Late Professor Westin directed research on the subject. Much of that research has since been represented in *"Privacy and Freedom,"* [35] a durable and exact writing, if any, on the subject of Privacy. In it, he wrote: *"[f]ew values so fundamental to society as privacy have been left so undefined in social theory, or have been the subject of such vague and confused writing by social scientists."* Years later, Westin's sentiment was echoed plainly by the moral philosopher Judith Jarvis Thomson, who said, *"[p]erhaps, the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is"* [36].

It is from such bounty of Privacy[22] and Security[23] conundrums that societal values are identified and formalized, frameworks for encouraging or discouraging social behavior are founded, and instruments of social justice, behavioral guidance, and punishment have been crafted. Foremost however, the situational inability to reconcile Privacy and Security conflicts in society stem from our limits of knowledge, the existence of false knowledge in these matters, and from our constant use of improper interpretations, techniques, tools, and services in relation to the area. A couple of analogously useful worldwide examples must be discussed to demonstrate the strength of this adversarial force.

## 2.2 Privacy knowledge boundary and its implications

In forewords to a 1970's seminal book on Privacy, then Chairman of the United States Senate Subcommittee on Constitutional Rights, U.S. Senator Sam J. Ervin, Jr., pushed for *"…all Americans to claim their constitutional legacy of personal privacy and individual rights and to demand an end to abuses of computer technology before the light of liberty is extinguished"* [37]. However, how is anyone to venture forward in attempts to put an end to "personal privacy" abuses, if one cannot rightly qualify and quantify privacy, as either a privilege or a right first, and/or if one cannot identify the correct lawful vehicles that one might use as a route to remediate one's loss of privacy, second?[24] Additionally, how is anyone able to hold those responsible for breaches in one's Personal Privacy and informational Security responsible? How is one to reclaim some semblance of that Privacy or Security lost, through the courts, when courts require "proof of harm," [38] and when such proofs are difficult to factually produce, or even forensically prognosticate beforehand, given that, those that were responsible for the breach may exploit the compromised information differently, and at during times, that are not immediately knowable, or mappable. Given the precarious nature of reclamations/repossessions of sensitive personal information and values associated, it is even more important to know, and to exacting details, one's privacy, and security profiles. If we are to follow-up on the Late Sam Ervin, Jr's advice to prevent "….*light of liberty [from being] extinguished,"* we have a long way to go to bridge the gaps in our knowledge to prevent Privacy and Security related encroachments.

How do any of us comprehend fully, the limits of our knowledge related to Privacy and/or Security? And, how are Privacy and/or Security knowledge limits likely to affect for instance, our ability to guard against the loss of Privacy and/or Security? To understand these questions better, and in terms of those contributions within the Special Issue, we must dedicate ourselves to dissecting a building block or two, in the steps involved in gaining mastery of knowledge. The first step in the process is to inspect/test our directional orientation. Are

[21] Emeritus Professor of Public Law & Government, Columbia University (USA)

[22] See above paragraph

[23] Provided here, as an example of the general state of the sector only. A Rustat conference report on cyber security at Cambridge University in which Sir David Omand GCB, Former Director of UK GCHQ was a participant, noted that, government intervention in aspects of the Cyber domain industry elements will likely be very necessary in situations where there is *"[u]nderreporting of criminal attacks by the private sector for PR reasons [which] leads to misunderstanding of the risks"* and in those situations where Cyber security industry is actively working on the *"reduction of negative externalities"*, that is to say: where commercial entities are engaged in actively pursuing short-term commercial gains while compromising long-term national security on the whole by opening-up compelling threats through short-sightedness. – Rustat Conference Report Cyber Security - An Assessment of the Threats to National, Economic and Individual Security, Rustat Conferences, Jesus College, Cambridge University, Cambridge, UK, Thursday, 3 February, 2011 https://www.jesus.cam.ac.uk/sites/default/files/inline/files/Rustat%20Conference%20Cyber%20Security.pdf AND Two thirds (66%) of UK SMEs queried did not consider their business to be vulnerable, and over three quarters (78%) of small businesses believed at least one major cybersecurity myth, which consequently placed their organizations at major risk. –The Rt. Hon. Karen Bradley MP, and Ed Vaizey, UK' Cabinet Office (Home Office); "Cyber security 'myths' putting a third of SME revenue at risk" [Misunderstanding of the threat posed by cyber crime is leaving SMEs vulnerable to losing information, profit and customers.] , UK Government (Whitehall), London, UK, 25 February 2015 https://www.gov.uk/government/news/cyber-security-myths-putting-a-third-of-sme-revenue-at-risk

[24] While examples relating to the United States are used herein, the relevance is universal

we oriented correctly, and do we have the building-blocks to the totality of the knowledge necessary?

### 2.3 How we presently view the world in which we live

This section intends to present to the reader that fundamentally, epistemological and ontological flaws - in that which we identify to be knowledge, will always holds us back from progressing rightly. How do we know, that which we have identified as being foundational to our knowledgebase is correct, and adequate, to be able to proceed ahead? This section asks that question of you – the reader, in a very basic way, by presenting for your consideration that the very world in which we have lived all our lives, has been incorrectly represented. Our "world view" as such, is essentially incorrect, unless you are viewing the Earth and the landmasses on a globe. Do you believe in the views that you possess of Privacy, and Security?

In "A History of The World in Twelve Maps," Jerry Brotton depicted the evolutionary history of World Maps in 12 steps [39]. Studying Brotton, one comes to understand at some level, his deeply held belief that a map "always manages the reality it tries to show*"* [40]. Brotton has performed a good service for the world of map inquisitors, noting that the evolution of maps of the world essentially depicts the desires of map producers to stage the powers of their respective States, colonial ambitions, or ambitions of empire etc. Albeit not cartographically, Privacy and Security perspectives have been expressed in ways and as part of people's morals, rituals, customs, system of laws, etc., along national and ethnographic boundaries; real or perceived. Map flavors, and the depictions of mapmakers as such, can be better understood for the intended purposes, if we consider at least two key bordering issues. **One** is to consider that which Siobhan O'Flynn has termed as a *"auto-topographic metanarrative"* [41]. In this case, it is humanity's need to articulate in some manner,[25] a close relationship to one's own "place", and one's "identity", but done so, in relation to the degree one senses to be "out-of-place" elsewhere, from being in contact with another race, culture, ethnicity, and gender. **The other** is to consider properly, the perspective offered by political scientist Jordan Branch. In "Mapping the Sovereign State: Technology, Authority, and Systemic Change" [42], Branch writes: *"[i]n the modern international system, both the character of states and their interactions are structured by exclusive territorial sovereignty" and accompanying "territorial authority"*… and *"…. new mapmaking technologies changed how actors thought about political space, political organization, and political authority. This change was fundamental to the creation of modern states and international relations, which were built around exclusive territorial sovereignty, discrete boundaries, and formal equality"* [43].

If observations by Branch were combined with those of O'Flynn and her *"auto-topographic metanarrative,"* [44] to represent one's own "place" and "identity" in relation to a sensing of how "out-of-place" one should be/is elsewhere, having come into contact with another race, culture, ethnicity, and gender, it is not a far stretch to envisage how value differentiations (such as personal valuations that we sense, and/or experience in relation to Privacy) could have become unaligned along topographical boundaries. It is as John Dee in the 1500s wrote in the leaves of the Preface to Euclid's *'Elements of Geometrie', "… some, for one purpose; and some, for another, liketh, loveth, getteth, and useth, Mappes, Charts and Geographical Globes"* [45]. Maps therefore, became a means to projecting or expressing professed differences between peoples, their societies, and their respective landmasses.

The Mercator projection[26] charted by Gerard Mercator in 1569 served any navigator well, and all else - improperly. Famously, the projection created the infamous "Greenland Problem," which, to this day, vulgarly misrepresents the geographic topography of the Continent of Africa against Greenland, when in fact, Africa is 14 times larger than Greenland (See Fig. 2). Despite the abundance of Space-Based Terrain Surveillance, Unmanned Aerial Vehicles (UAVs) and satellite based observational platforms, and an extensive mapping of the Earth's surface by satellite over many decades, Google-Maps and Microsoft's Bing-Maps still utilize the nearly 500 year old Mercator Projection, continuing to electronically propagate existing errors in the way people perceive our living world.

In a similar fashion, the silhouettes and curves of Privacy vary across cultures and landmasses, not merely for want of clarifications, and precision in definitions, but also for a better understanding of Privacy's value - in relation to Universal Human Rights. In the *"Have Distortions Will Travel"* department, is the odd case of Google, and the way in which Google Maps represent disputed areas of the world for specific populations, and on the fly, reflective of a country's central government policy on geographical disputations [46]. It has been reported that in at least 12 regions of the world, Google presents national border representations dissimilarly, based entirely on where the search/audience is located. Seeing that "Google Maps has the most comprehensive map set, and the largest map readership in the world (still) —with a billion users each month" [47], serving-up such customized geographic representations amount to the opportunity to continue propagating errors, at a rate of 1 billion times a month.

These examples simply serve to signify to the reader that each of us, more than less, believe we are seeing the world as it really is, when we are not. Such is the case with Privacy and

[25] Maps in this case

[26] A Projection is the means by which the 3 dimensional surface of the Earth is represented on a 2 dimensional plane

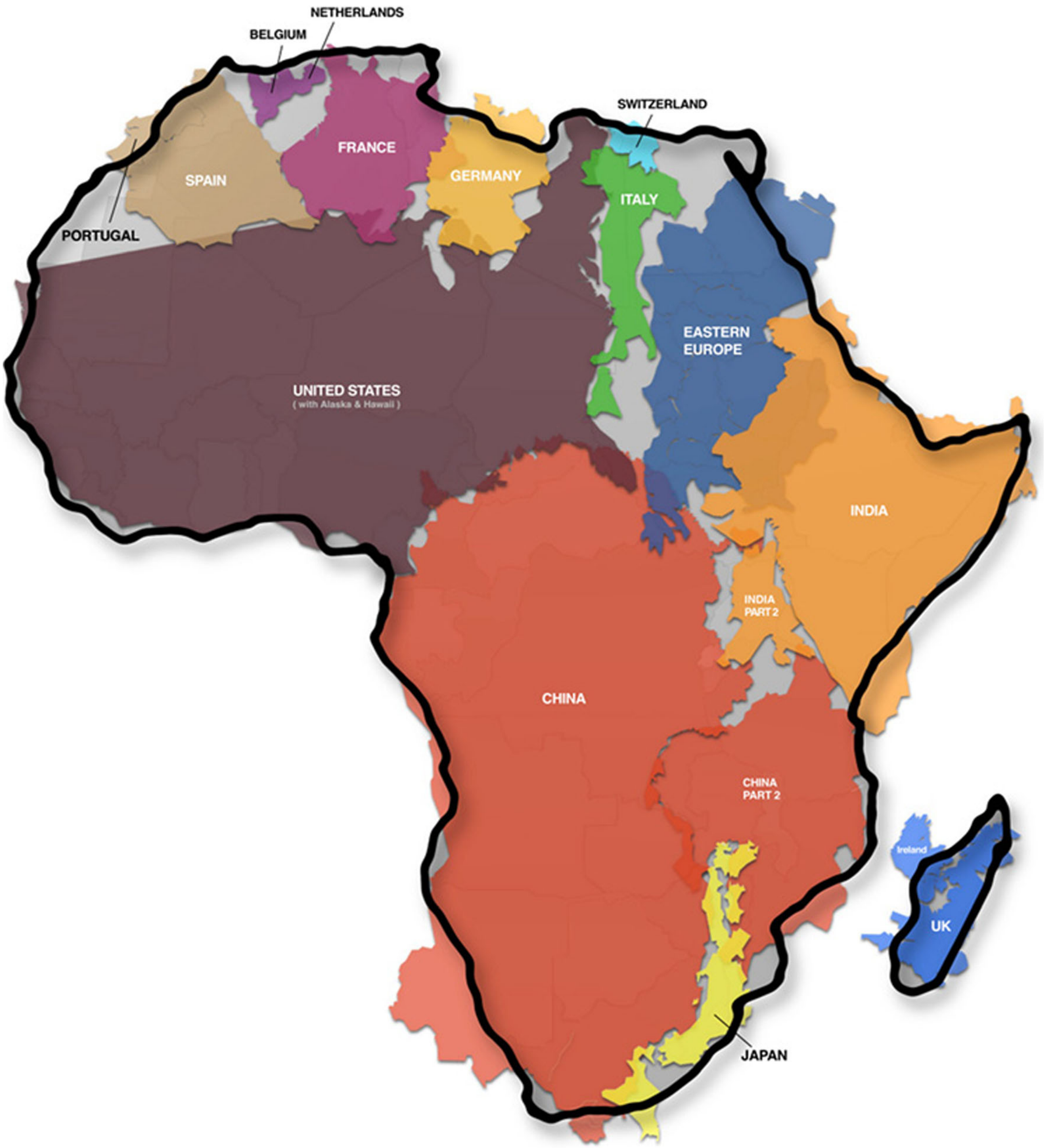


**Fig. 2** An Amended Depiction of Long-Standing Distortions Concerning Geographical Proportions of The African Continent. Kai Kraise; “The True Size of Africa: A Small Contribution In The Fight Against Rampant Immappancy”, January 2015

Security also. Consider disputed northern areas of India as an ideal example where incongruity of visuals is well represented.

Northern-most to the Indian Sub-Continent are certain disputed areas; some of which China claims, and another that Pakistan claims. Given these disputes, if anyone performs a map search on India, from India, Google Maps proceeds to present the entire Indian Sub-Continent as having ‘normal international boundaries with Pakistan and China.’ On the other hand, if one were to perform the same search, from either Pakistan or China, the Indian Sub-Continent and the disputed northern areas are presented having mutual borders that ‘are in dispute’, with both Pakistan and China; in a manner that reflects the internal view from each country. For instance, if one performs a search related to Indian territories from inside China, the disputed territory is drawn by Google Maps as a territory that is a part of China (See Figs. 3, 4, and 5). Why is this, and other actions such as these, important? It is perhaps understandable that Google as a “vendor,” to curry favor with the central government of a nation, could/would represent information in a way that is congruent with central government ideology. How is the receiver of the represented information to determine - what is correct and appropriate? Similarly, and analogously, there are many trans-national Privacy views, which are not harmonious with others[48].

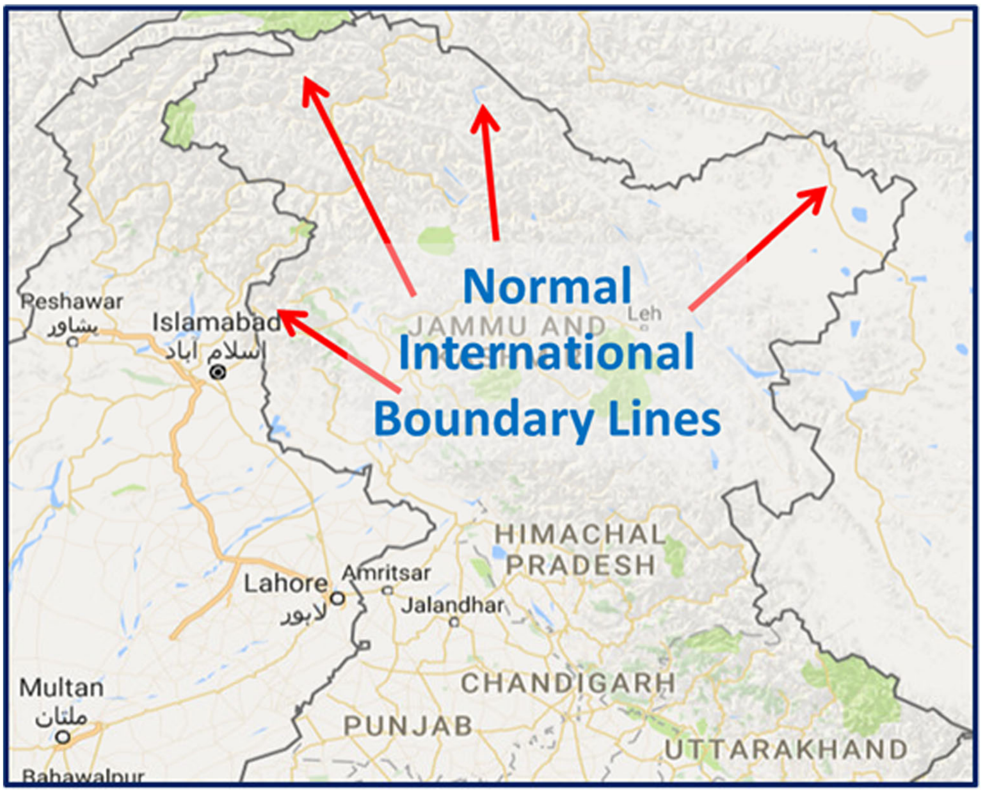


**Fig. 3** Disputed Northern Indian Territories As Seen From Inside India

Aside from propagating errors, in this case, consider that the U.S. Intelligence Community identifies the northern territory of Kashmir as *the site of the world's largest, and most militarized territorial dispute* with portions under the de facto administration of China (Aksai Chin), India (Jammu and Kashmir), and Pakistan (Azad Kashmir and Northern

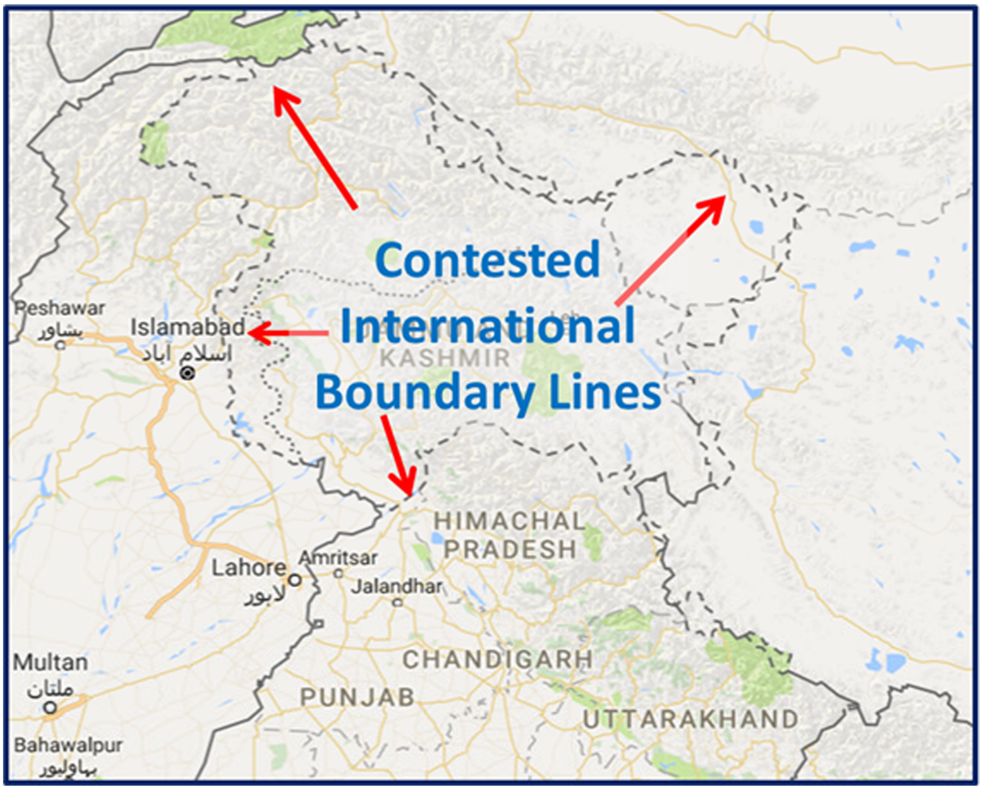


**Fig. 4** Disputed Northern Indian Territories As Seen From Pakistan & Others Outside India, Except China

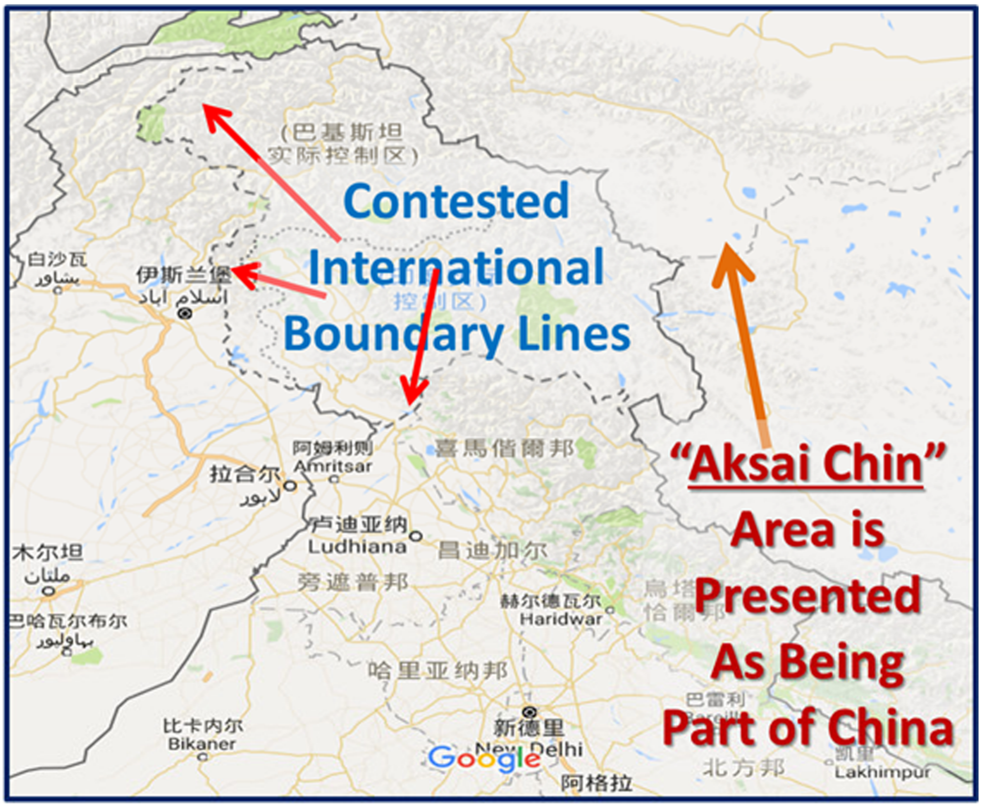


Fig. 5 Disputed Northern Indian Territories As Seen From Inside China

Areas).[27] Therefore, from purely an educational point of view, will it be important for those curious geo-politicos, to understand the fine points of the contention among three nuclear powers? Why this discussion of Maps?

Firstly, the similarity in *the nature of the muddles* caused by the map errors, and the related implications generate a larger "*influence,"* that is truly global in nature, and intergenerational in its extent. Secondly, the effects of interpretive errors, in how we view our world, experience it, and then possibly continue to propagate views in error – *assist to entrench and cement* corrupted cultural, economic, political, geo-political views, even to the extent that such views can worsen the standing (friendly/adversarial) relations with nation states and their respective populations. In short, without proper geographical knowledge, we cannot comprehend, to the extent needed, the "crises" and the series of flourishing chaos in places such as the Syrian Arab Republic, Occupied Palestinian Territory, The Sahel, The Democratic Republic of The Congo, Nigeria, Chad, Ethiopia, Somalia, Kenya, South Sudan, Iraq, Yemen, Libya, Afghanistan, Myanmar, or the Philippines.[28] Lastly, and again, views related to Privacy and Security also have similar taints, which must be corrected before proper Privacy protections and Security configurations can be instantiated.

## 3 High political entanglements and the subjugation of privacy and security

Entanglements are referred to herein as quagmires of a moral, or an ethical nature; or a consequence created by an action of government, such as a political enactment that inflicts a destroyingly cleaving effect on all surrounding things, including in this case, Personal Privacy and the Security of persons. Moral prevarication in society creates ethical quandaries; and ethical quandaries created, then make it possible for us to easily violate the Personal Privacy or Personal Security of another. This section will attempt to demonstrate to the reader, the need for 'universality' surrounding the ideas and ideals of Privacy and Security. Drawing upon certain thought-provoking cases, the author will attempt to demonstrate to the reader for instance, how and where - the once oppressed, was able to turn into "the subjugator," or at least be a facilitator of subjugation of others. The reader is to gain thereby, an appreciation for the wide-ranging types of entanglements, societies are capable of creating, and under what circumstances such entanglements are sustained, causing a depletion of Personal Privacy and Security for all.

Ultimately, the section is a reveal to the nature of human corruptions that affect Privacy and Security of persons directly, and the greater need for the civilizing of man; a need for universal calibration of our moral and ethical compasses. C.*S. Lewis* once said:

[27] Source: U.S. Central Intelligence Agency, August 1, 2017

[28] Source: Areas of Sustained Conflicts, UN Office for the Coordination of Humanitarian Affairs (OCHA), Geneva, August 2017

> "We all want progress. But… if you have taken a wrong turning, then to go forward does not get you any nearer. If you are on the wrong road, progress means doing an about-turn and walking back to the right road; and in that case the man who turns back soonest is the most progressive man… We are on the wrong road. And if that is so, we must go back, Going back is the quickest way on."[29]

There are entirely too many 'Privacy and Security' related misfortunes that humanity has brought about, and by way of the quagmires created, which we have then assisted to escalate, and to intensify. Despite the amount of time that has passed, and in full view of painful histories, those same histories have near-faithfully repeated. Therefore, at least within the greater context of presentations within this Special Issue dedicated to Privacy and Security these histories deserve a brief mention. Individual knowledge, combined with individual awareness, and a very personal desire to act upon that knowledge and awareness combination, can result in "the quickest way on," toward progress.

It is frequently presented that a government has the right to collect information on citizens for the betterment of societal welfare all around. History has also proven it true that collected information by government is not always used correctly; in fact, governments of the United States, China, Germany etc., have abused "the confidence," "expectations," and "charge"[30] of Citizens [49]. In view of such corruptions and turbulent government-citizen relations, can citizens be certain, and at any time, that government use of collected citizen information will be strictly confined to purposes originally stated when information was first collected, and would thereafter be accessed or distributed only by those individuals who have an 'oath-borne' and legally clarified and bounded responsibility to access such information?

At present, no government in the world supplies their citizens with concrete assurances and corresponding recourses (in case of offenses) against any of the information that government collects, and that which may become compromised later. Even Estonia, that nation known to be the world's first *e-Society,* has yet to fully comprehend, and confront the range of digital insecurities that can prospectively inflict that state. The State of Estonia has neither the type, or the scale, nor the specialized and defined expertise and resources necessary to defend against, or to quell the nature and the possibilities of threat vectors. Just one such threat example that could affect Estonian e-Society was made clear recently, which has required the Estonian State to revoke all State issued Digital E-Certificates beginning in late 2014 [50]. The Estonian Public Broadcaster reported in October of 2017 that, "[o]n Aug. 30, an international group of researchers informed the RIA[31] that they had discovered a security risk affecting all ID cards issued in Estonia beginning in Oct. 2014, including ID cards issued to Estonian e-residents. Nearly 750,000 ID cards are affected by the issue*"* [51]. The Estonian Public Broadcaster also noted the Head of the Estonian Police and Border Guard Board's Identity and Status Office (PPA)[32] saying that, *"[i]n the event that there is sound evidence that the risk (digital certificate compromise) has materialized, the PPA as the issuer of the document will revoke the certificates of all the cards affected by the security risk"* [52].

Since the original notification of the security risk to the Government of Estonia in August, the government identified 136 critical services nationwide that would be affected by the reported security risk; 44 of 136 critical services were deemed high priority [53]. As of late, the Government of Estonia determined that it is best to invalidate all Digital Certificates (issued since Oct 2014) in circulation and use; in healthcare, in government service, and in general life, than to risk widespread compromises [54]. Still, globally, risks will remain persistent, and pervasive, in such areas as Healthcare, Banking and Finance [55], for systems and vulnerabilities are not well scoped, or understood. The reader is reminded that Estonia's recent decision to withdraw digital certificates represents just one threat example that nationally deployed government controlled systems will face, in the present and the future, and those that the likes of U.S. Government is presently considering deploying in the United States. From Argentina to Ukraine and to Zimbabwe, identity and identification systems are in place that can suffer serious compromises, and governments have little inhouse abilities to prevent breaches of their systems.

The hazardous informational breach of the United States Office of Personnel Management (OPM) represents a prime example of a government system compromise, where there exists no possible way for the millions of Americans whose most sensitive information have been compromised to be able to seek legal restitution. Some of the most sensitive types of information collected on various persons to whom the United States Government has granted Clearances (so that such persons may then handle sensitive government information on behalf of the government in the course of their duties), has fallen into the hands of those who compromised OPM's Systems. Even if somehow, culpability in relation to the OPM systems breach could be asserted, and some type of financial restitution for the breach of highly sensitive information belonging to millions of Americans could be made, how could anyone still prevent the use of the information that was stolen?

The type and scale of information kept on people with clearances by the U.S. Government are of a nature that is incredibly more sensitive, and incredibly more invasive than any credit bureau file kept on the same people. Essentially, the only recourse in

[29] Lewis, Clive Staples; "The Essential C.S. Lewis" In: "We Have Cause To Be Uneasy", Touchstone/Simon & Schuster, New York, NY, 1996

[30] These characteristics are used here in the place of the widely used and abused term "trust"

[31] Information Systems Authority - Government of Estonia

[32] Margit Ratnik – Head, Structural unit: Police and Border Guard Board - Development Department, Identity and Status Office https://www.politsei.ee/en/kontakt/teenistujad/teenistuja.dot?pid=564554

relation to the breach of sensitive information amounts to Credit Monitoring by Credit Bureaus. The reader must be informed that the OPM intrusion is not well represented or discussed [56]. That said, we are now on to the Equifax breach, which, as a company is now responsible for having left bare the credit files on what is now known to be 145 million Americans. For what it is worth, Equifax is also one of the companies responsible for offering Credit Monitoring services in relation to the OPM breach.

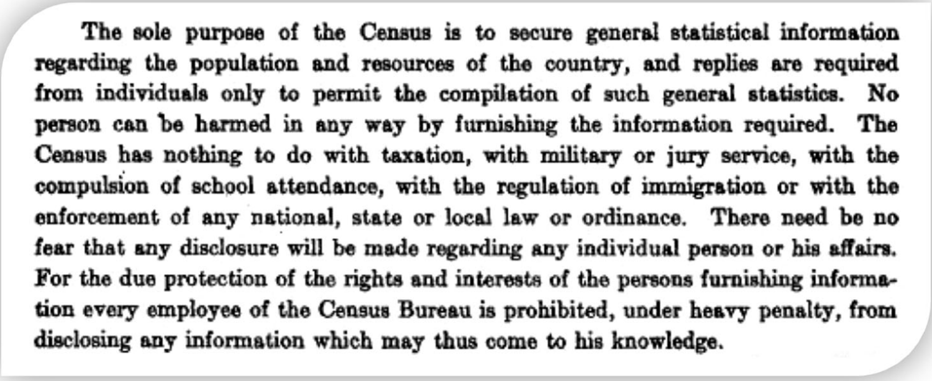
What is the *"knee-jerk-reaction"* from the wise representatives of the people on such matters? Get rid of Social Security numbers! [57] Let us understand somethings that are quite fundamental to the issue. U.S. Social Security numbers were to have never been used as identifiers, for any other purpose than those originally deemed to have been necessary to fulfill those purposes of the U.S. Social Security Administration (SSA). Second, getting rid of Social Security Numbers from its widespread Public & Private usage will not strengthen any 'weak and poorly administered system' that is presently deployed in the field. Elimination of Social Security Number use within U.S. Public and Private sectors will not, and cannot rid systems of their most fundamental "people-process-technology" flaws. Besides, one of the key things that the United States needs (as do many other countries), is comprehensive data protection regulations and enforcement, that is neither half-baked, nor one that mimics another circus of fools. [58].

On another note, and to be certain, it is being emphasized here to the reader that Equifax was notified 6 months prior to the now "publicized" time of compromise, that their systems were vulnerable [59]. The Fmr., and current CEOs of Equifax CEO appeared before U.S. Congress to report that they are vulnerable, and cannot prevent attacks launched against it by Nation States [60]. It is not at all clear that Equifax was breached by a Nation State. Just the same, how could Equifax be prepared to defend against anyone, or any type of an informational breach, attempted by anyone, when the company blatantly failed to act even minimally, on key warnings of systems vulnerabilities being present, months before the system compromise?

The former CEO of Yahoo!, Marissa Mayer testified before the same Congressional Committee, as did the Equifax personnel, stating before the Committee that, even stronger corporate information system defenses cannot stop breaches that are attempted by sophisticated and persistent actors [61]. If this is so, why then was a scrapping of 'Social Security Number use' discussed by the Committee at all? What was the purpose? The inconceivable naïveté, and the mind-boggling opacity that tech CEOs, lawmakers and regulators display on such matters, especially in light of the fact that tech companies, lawmakers and regulators represent a nucleus behind "public-private" partnerships and engagements that are routinely seen to be working on emerging prospective avenues of protecting the public – is at the very least, tragic. Lastly, on this subject, Equifax was as of recent, and as 'arsTECHNICA' made note of it, "borked again*"* [62]. This time, visitors were exposed to a possible *Malvertising* (Malware in an Ad) campaign during a visit to the Equifax web site. The range and scope of ***institutional failures***[33] that permit such extensive deficiencies in moral, and ethical accountabilities, and operational competence in companies, is not surprising.

## 3.1 In the land of the free, home of the brave – the interned

Before the taking of the 15th Census of the United States, then President Herbert Hoover proclaimed: [63].



The sole purpose of the Census is to secure general statistical information regarding the population and resources of the country, and replies are required from individuals only to permit the compilation of such general statistics. No person can be harmed in any way by furnishing the information required. The Census has nothing to do with taxation, with military or jury service, with the compulsion of school attendance, with the regulation of immigration or with the enforcement of any national, state or local law or ordinance. There need be no fear that any disclosure will be made regarding any individual person or his affairs. For the due protection of the rights and interests of the persons furnishing information every employee of the Census Bureau is prohibited, under heavy penalty, from disclosing any information which may thus come to his knowledge.

Hoover's pronouncements upon U.S. Government's then installed measures safeguarding Census information then, and since, have rung hollow. As Anderson and Seltzer have noted, despite several such Presidential

[33] Conveying explanations relating to the concept of *"Institutional Failure"* is largely beyond the scope of this writing. As an example however, the reader is introduced to: "The Consequences of the Global Financial Crisis: The Rhetoric of Reform and Regulation" [Wyn Grant and Graham K. Wilson, Eds.], Oxford University Press, Oxford, UK, 2012

Proclamations, U.S. Census Directors, who served Presidents from both major U.S. political parties have violated Presidential proclamations, having inked lawful guarantees [64]. Anderson and Seltzer also concluded that, "interagency pressures and perceived national security needs" [65] imposed upon the Census Bureau – launched the violations that led to the internment of Japanese-Americans in droves (See Figs. 6 and 7).

If Census Directors were bound by law, and clear, lawful prohibitions in purveyance and exploitation of Census data were in existence, how is it that a Census Director, appointed to protect persons from harm under heavy penalty (judging my Hoover's Proclamation) can effortlessly succumb to "interagency pressures and perceived national security needs" and violate the Privacy and Security of persons? Authors of "The Dark Side of Numbers The role of Population Data Systems in Human Rights Abuses," [66] claim that *bureaucratic opportunism* and *professional zeal* were to blame for Privacy and Security violations; which indicates to this author – the common occurrence of pre-meditation, as associated with *bureaucratic opportunism* and *professional zeal* do not logically complement 'interagency pressure' and 'national security need.' Besides, official excerpts from Census Bureau conversations from 1942 places then Census Bureau Director J.C. Capt as a willing participant, and who, according to Seltzer and Anderson, is known as having said, *"We're by law required to keep confidential information by (sic) individuals. But in the end, [i]f the defense authorities found 200 Japs missing and they wanted the names of the Japs in that area, I would give them further means of checking individuals"*… [67] And Capt is noted to have also said that, *"[t]hose who got [Census Data] thought they were pretty valuable. That is, if they knew there were 801 Japs in a community and only found 800 of them, then they have something to check up on..."* [68].

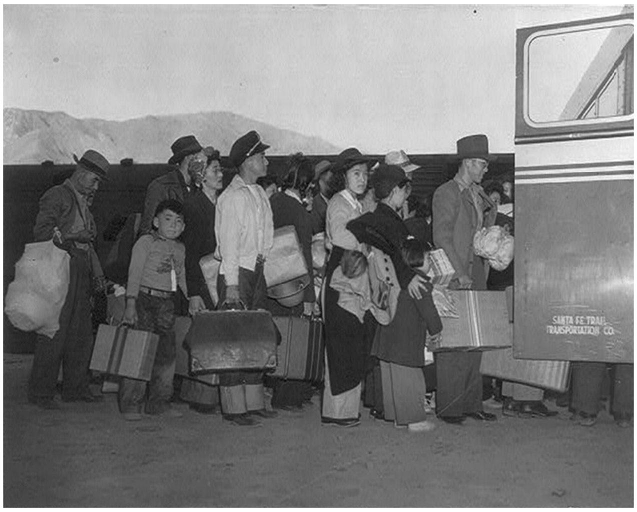
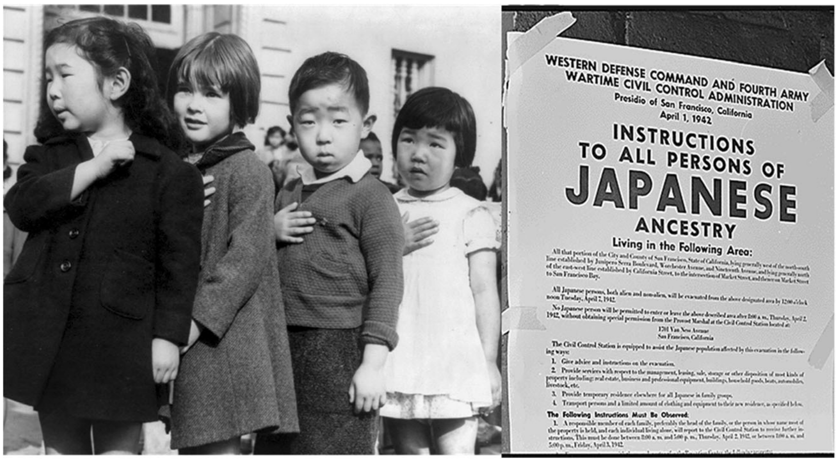


**Fig. 7** Japanese-Americans transferring From Train to Bus at Lone Pine, California, Bound for 'War Relocation Authority Center' at Manzanar. Source: U.S. Library of Congress

By the aforementioned statements alone, any reader could characterize then U.S. Census Director Capt, and the staff under his supervision as being "motivated" to violate the law, and to acquire full details of all the people who were Japanese, or of those who were Japanese-American. Naturally, later research has revealed that Census Bureau did violate law and hand over confidential data on Japanese-Americans to the United States Secret Service [69]. Much later, when the information of the violation became public, Christa Jones, the Chief of the Office of Analysis and Executive Support at the U.S. Census Bureau seemed to provide assurances that the 'present-day' Bureau cannot use the information as it once did, and that stronger protections are in force at present. The Los Angeles Times cited Jones as saying, "[i]t's our commitment to protect the confidentiality in everything we do*"* [70]. Perhaps, in saying this, Ms. Jones was hoping that

**Fig. 6** Some First-Graders of Japanese Ancestry - Weill Public School, San Francisco, California Pledging Allegiance to the United States. They Were Soon Interned For the Duration of WW-II. Source: U.S. Library of Congress



WESTERN DEFENSE COMMAND AND FOURTH ARMY
WARTIME CIVIL CONTROL ADMINISTRATION
Presidio of San Francisco, California
April 1, 1942

INSTRUCTIONS
TO ALL PERSONS OF
JAPANESE
ANCESTRY
Living in the Following Area:

All that portion of the City and County of San Francisco, State of California, lying generally west of the north-south line established by Junipero Serra Boulevard, Worchester Avenue, and Nineteenth Avenue, and lying generally north of the east-west line established by California Street, to the intersection of Market Street, and thence on Market Street to San Francisco Bay.

All Japanese persons, both alien and non-alien, will be evacuated from the above designated area by 12:00 o'clock noon Tuesday, April 7, 1942.

No Japanese person will be permitted to enter or leave the above described area after 8:00 a. m., Thursday, April 2, 1942, without obtaining special permission from the Provost Marshal at the Civil Control Station located at:

1701 Van Ness Avenue
San Francisco, California

The Civil Control Station is equipped to assist the Japanese population affected by this evacuation in the following ways:

1. Give advice and instructions on the evacuation.
2. Provide services with respect to the management, leasing, sale, storage or other disposition of most kinds of property including: real estate, business and professional equipment, buildings, household goods, boats, automobiles, livestock, etc.
3. Provide temporary residence elsewhere for all Japanese in family groups.
4. Transport persons and a limited amount of clothing and equipment to their new residence, as specified below.

**The Following Instructions Must Be Observed:**

1. A responsible member of each family, preferably the head of the family, or the person in whose name most of the property is held, and each individual living alone, will report to the Civil Control Station to receive further instructions. This must be done between 8:00 a. m. and 5:00 p. m., Thursday, April 2, 1942, or between 8:00 a. m. and 5:00 p. m., Friday, April 3, 1942.

those with historical knowledge and memory would overlook, or simply gloss over the facts, that despite Presidential Proclamations and 'protective Laws-in force' against harm in the use of Census information collected by U.S. Government, Japanese-Americans were interned; and that internment cost many, their life foundations; their homes; their businesses/farms/trades, and all means by which they and their families could be sustained. U.S. Government reparations for the internment - came along "too little, and too late." At the time, Ms. Jones was also heard saying that under a "War-footing," sharing of such information was legal. These and other such *contradictions issued by sycophantic and unlearned bureaucrats* should never be considered by citizens as being assurances of available protections. As the reader, you will have to make the decision to whether any government can, or will, under the premise of *exigent circumstances,* invade your Personal Privacy and/or Security. In light of all that has been revealed by Edward Snowden in the post 9/11 era, many government actions have been very telling.

During his tenure, Kenneth Prewitt, Fmr. U.S. Census Bureau Director (1998 to 2000) issued a public apology to the American people (an action no other Census Director has done, before, or since) for the misuse of Census information. In a review of the new research evidence, which Prewitt claimed to be *"a remarkable piece of historical detective work,"* [71] he also said, *"[a]t the time, available evidence (and Bureau lore) held that there had been no ... release of microdata .... [t]hat can no longer be said"* [72].

### 3.2 Thomas J. Watson's Lagniappe to a 1000 year Reich

International Business Machines (IBM), perhaps once most powerful American archetype of an information technology company may very well be noted by historians as having ushered in the modern Surveillance State. IBM, through its German subsidiary DEHOMAG, sold Hollerith Card devices to Germany, to the nationalists, who then proceeded to use that technology with the explicit knowledge and assistance of IBM-HQ and Thomas J. Watson, its Chief Executive, to near mechanized perfection; a state sanctioned killing machine that ultimately claimed the lives of more than 6 million human beings. As Edwin Black has assembled in his well-researched work on IBM's involvement in murderous activities of the National Socialist Party in Germany, IBM systems and methods did not simply track prisoners in massive camps, but aided in the management of the entire camps through instrumented camp logistics governed by IBM technology.

As Black has noted, on any given day, total camp population was ~700,000, which required IBM's technology and methods for population management. And as *"slaves within camp confines died or reached the limits of their utility to the Reich the prodigious task of efficiently scheduling deportation from cities and ghettos in many countries, the daily work assignments, and outright extermination timetables would have been impossible without the daily strength reports"* [73]. These described tasks fell to IBM's Hollerith technology and methods (See Fig. 8).

In a bizarrely spun, morally disinfected, and innocuous sounding statement, Willy Heidinger, DEHOMAG's German Executive is cited as having made the following remark, upon the inauguration of a DEHOMAG center in Berlin, in January of 1934. Heidinger is cited saying. *"[t]he physician examines the human body and determines whether… all organs are working to the benefit of the entire organism."* ... *"We [Dehomag] are very much like the physician, in that we dissect, cell by cell, the German cultural body. We report every individual characteristic… on a little card. These are not dead cards, quite to the contrary, they prove later on that they come to life when the cards are sorted at a rate of* ***25,000*** *per hour according to certain characteristics. "These characteristics are grouped like the organs of our cultural body, and they will be calculated and determined with the help of our tabulating machine"… "We are proud that we may assist in such task, a task that provides our nation's Physician [Adolf Hitler] with the material he needs for his examinations"* [74].

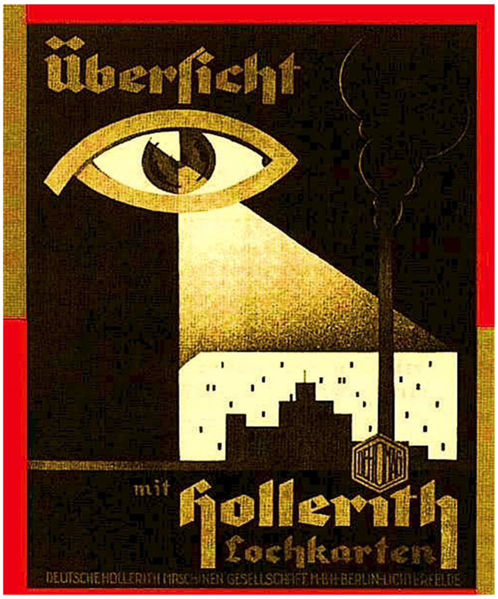

überſicht
mit
hollerith
Lochkarten
DEHOMAG
DEUTSCHE HOLLERITH MASCHINEN GESELLSCHAFT M.B.H. BERLIN-LICHTERFELDE

**Fig. 8** The **"All Seeing"** State *"Beyond Fences," It Says, "With Hollerith Punch-Cards"* (DEHOMAG) Source: Drawn from Pubic Domain and Incorporated Into Author's Privacy Presentation for IFMBE – Global Citizen's Safety & Security WG Session, IUPESM World Congress 2015, Toronto, Canada

Yes, indeed, no Hollerith card was dead then, as Heidinger had told, when their journey began. Ultimately though, each card served the *Reich* to strip every ounce of usable energy, in every person to benefit an 'evil' and 'crumpled' vision of immortality forged by a madman – until the very last breath every person had, was exhausted.

Captivating are the details of IBM's operational history during this period as investigated and corroborated by Black; it indicates a very sinister moral compass at the core of IBM, at the core of its chief-man: Watson. Black discovered that as Hitler carved and pillaged through Poland, Holland and Vichy France, IBM had followed, and in some cases was there first – in anticipation of carrying on, the business of carrying on. As Black further notes through research, when signs of atrocities toward the Jewish people were all around, IBM simply turned a blind-eye to all of it, where the order of the day was *"don't ask, don't tell"* [75]. In reality, as Black notes, Thomas Watson's personal representatives *"were almost constantly in Berlin or Geneva, monitoring activities [in Germany], ensuring that the parent company in New York was not cut out of any of the profits or business opportunities Nazism presented"* [76].

IBM profited tidily from a business that was fundamentally padded with money that came from giving support to State sanctioned terror and Murder enterprise operations, designed to dispossess every targeted man, woman and child, of their dignity, humanity and, at last, their life [77]. The deprivation that people experienced, where they lost their personal Privacy and their personal Security were, in the scheme of things, minimal, when considering their pre-ordained fate; death by IBM Punch-Cards. Finally, Black determined that *"IBM's business was never about Nazism. It was never about anti-Semitism. It was always about the money. Before even one Jew was encased in a hard-coded Hollerith identity, it was only the money that mattered. And the money did accrue"* [78].

In reviewing these examples, the author is in no manner implying that national security needs of a State are unimportant. As a State, at any time, if State instruments - either singularly, or collectively ceases to concern itself with the very purpose of its existence (service to the people), and principles (Constitution) by which it/they are made to exist, then it is time to re-calibrate structures, and re-direct and/or re-purpose the personnel within them. Old Germany represented a different case, where extermination of a group of people was the objective of the State, here, the major point of concern is that terror enterprises such as the *Reich*, almost always, cannot operate without assistance. In this case, IBM provided the critical component; the training, and support for the component – to keep the terror enterprise humming effectively and efficiently.

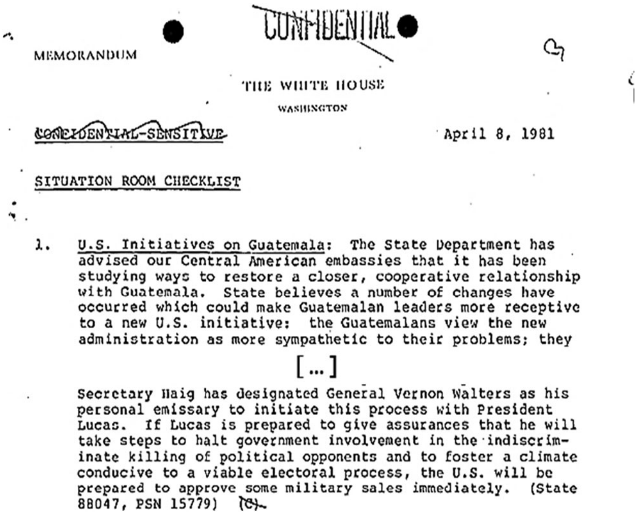
### 3.3 The case of Guatemala: where, the once oppressed, gamely facilitated brutality

On 20 May 2015, a lynch mob consisting of ordinary Guatemalans gathered outside the Municipality of Rio Bravo in Suchitepéquez Department (County). The mob got hold of a 16 year old girl suspected of having had a hand in the murder of a 68 year old taxi driver, the crowd then encircled the 16 year old, proceeded to beat her brutally, doused her with petrol, and burnt her alive, all while the crowd of adults and the young stood by watching [79]. According to INACIF, the Guatemalan National Institute of Forensic Sciences, between the month of January and May of 2015, there were 2343 murders in Guatemala. The land area triangulated by El Salvador, Guatemala, and Honduras is now the most violent non-war zone in the World. Why is it essential to discuss this matter in relation to Privacy and Security of citizen information? The point of great importance to present and discuss in terms of Guatemala and elsewhere is: if anyone has chosen to not respect human life that same party could not ever be expected to be respectful of the "human rights" of others. Secondly, it is important to discuss the happenings in Guatemala, and the background to those happenings, as they are both necessary to discuss the evolution of surveillance states in modern times. Additionally, Guatemala and certain other Central American nations were in essence 'groomed' or 'developed to be' the violent states they are now, over a period of time, and are fundamentally organized to be antithetical to Privacy and Security values.

Guatemala, once at the center of the glorious Mayan Civilization, is now an environment not alien to total communal violence. Guatemala suffered extensive mutilations by a civil war that raged on for more than **30** years. Guatemala is a country where 'extreme close contact violence' inflicted by one despot after another upon the people, entrenched and widely-spread, institutionalized corruption, failed institutions of governance etc., all of which nurtured the growth of a societal degeneration, which has shaped the likes of that savage killing of the 16 year old as stated before, insensitivity to human life, and lawlessness. The author's intention here is to assist the reader in the realization that semblances of Personal Privacy and Personal Security are dependent on so much more than the mere existence of Data Privacy and Security laws. An examination of situations as they have been in existence in Guatemala will afford yet another rich indicator to the reader, of the need for solid societal foundations for Privacy and Security. To make matters of discussion related to Privacy and Security more suited to the reader in terms of Guatemala, and the rest of the world, the author intends to demonstrate in brief, how certain seeds of societal destruction were sown, and how all are now reaping its harvest.

Viron Vaky was once United States' Deputy Chief of Mission (DCM)[34] in Guatemala. Upon his return to the States, and re-assignment to the Policy Planning Staff (S/P)[35] at the Department of State's Policy Planning Council, Vaky wrote a Classified and candid memo to Covey Oliver, then Assistant Secretary of State for Inter-American Affairs, regarding observations on happenings in Guatemala since his departure as DCM, and of U.S. Involvement in Guatemala. In the memo, which has since been Declassified, Vaky is seriously troubled by the ostensibly perpetual actions by Government of Guatemala (GOG), and of U.S. culpability in it. Vaky defined the actions being taken by GOG as having a *"terribly corrosive effect on Guatemalan society and the nation's political development"* (See relevant excerpts from the Vaky memo in Appendix). Vaky stated, and with bluntness not usually seen, to Oliver that, continued GOG actions have *"just deepened and continued the proclivity of Guatemalans to operate outside the law. It says in effect to people that the law, the constitution, the institutions mean nothing, [and] the fastest gun counts"* (See Appendix). In other words, Vaky was informing Oliver that the U.S. was helping to groom a lawless society. In 1977, citing the continued prevalence of horrendous human rights violations, the Carter Administration in the U.S. pulled-back, and in fact, ceased supplying Guatemala with arms.

Since Vaky dispatched his concerns and critique of U.S. engagements with Guatemalan entities and of in-theatre events in 1968, to have it served-up to U.S. Secretary of State Dean Rusk in a Policy context, still other flows of (then) Classified reports from both the U.S. Embassy in Guatemala, the Central Intelligence Agency (CIA) and the Defense Intelligence Agency (DIA) came into U.S. Government in Washington, regularly, relating the brutality of the violence, extrajudicial killings, political murders and corruption among other things. However, immediately after Ronald Reagan became the President of the United States, succeeding Jimmy Carter, both Reagan and his administration wanted to, as quickly as possible, restore military aid and training to the repressive Guatemalan Government that was killing its citizens in the name of fighting communism. And eventhough a steady stream of information was coming in from the field - into the possession of the Reagan Administration, 'retelling tales of horrors,' internally advising continually, 'no involvement' with Guatemala, the White House secretly made overtures to Guatemalan officials of the new administration's desire to want to support (See Fig. 9). Regan's own Ambassador to Guatemala, Frederic L. Chapin, by way of giving a status report in February of 1984, urged Secretary of State George Shultz to take the moral high ground (See Fig. 10), asking as Vaky did in 1968, to ponder upon our (U.S.) values and to not be 'duplicitous' on Guatemala, given the barbarism on the ground; to no avail.



CONFIDENTIAL

MEMORANDUM

THE WHITE HOUSE

WASHINGTON

~~CONFIDENTIAL-SENSITIVE~~ April 8, 1981

SITUATION ROOM CHECKLIST

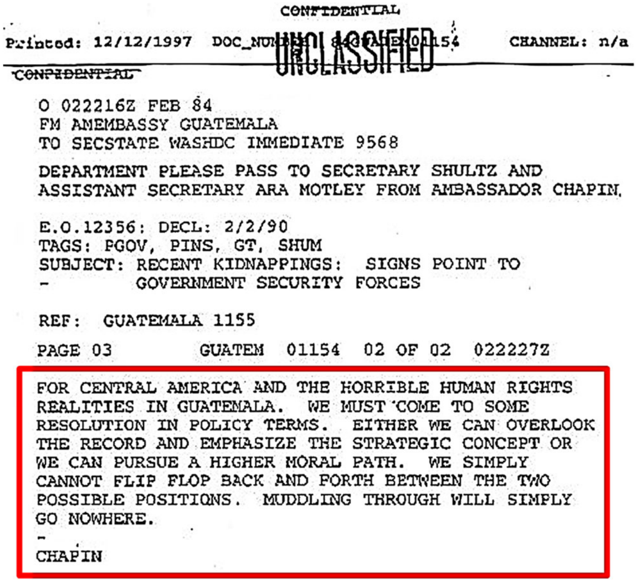
1. U.S. Initiatives on Guatemala: The State Department has advised our Central American embassies that it has been studying ways to restore a closer, cooperative relationship with Guatemala. State believes a number of changes have occurred which could make Guatemalan leaders more receptive to a new U.S. initiative: the Guatemalans view the new administration as more sympathetic to their problems; they

[...]

Secretary Haig has designated General Vernon Walters as his personal emissary to initiate this process with President Lucas. If Lucas is prepared to give assurances that he will take steps to halt government involvement in the indiscriminate killing of political opponents and to foster a climate conducive to a viable electoral process, the U.S. will be prepared to approve some military sales immediately. (State 88047, PSN 15779) ~~(C)~~

**Fig. 9** Reagan White House Action Items. Source: Ronald Reagan Presidential Archives

Back in 1977, when the Carter Administration ordered a U.S. military assistance pull-back, an arms-sales vacuum was created, and Guatemala did not have to look for long to have the void filled, for it was very speedily and happily filled by Israel, who had a growing defense industry to maintain, beginning in 1967. Beyond Israel's arms sales, the country provided technology transfer and technical assistance too. In "Israel and Latin America: The Military Connection," Bahbah and Butler record that *"the importance of Israel's*



CONFIDENTIAL

Printed: 12/12/1997 DOC_NU[illegible]154 CHANNEL: n/a

UNCLASSIFIED

~~CONFIDENTIAL~~

O 022216Z FEB 84
FM AMEMBASSY GUATEMALA
TO SECSTATE WASHDC IMMEDIATE 9568

DEPARTMENT PLEASE PASS TO SECRETARY SHULTZ AND ASSISTANT SECRETARY ARA MOTLEY FROM AMBASSADOR CHAPIN.

E.O.12356: DECL: 2/2/90
TAGS: PGOV, PINS, GT, SHUM
SUBJECT: RECENT KIDNAPPINGS: SIGNS POINT TO
- GOVERNMENT SECURITY FORCES

REF: GUATEMALA 1155

PAGE 03 GUATEM 01154 02 OF 02 022227Z

FOR CENTRAL AMERICA AND THE HORRIBLE HUMAN RIGHTS REALITIES IN GUATEMALA. WE MUST COME TO SOME RESOLUTION IN POLICY TERMS. EITHER WE CAN OVERLOOK THE RECORD AND EMPHASIZE THE STRATEGIC CONCEPT OR WE CAN PURSUE A HIGHER MORAL PATH. WE SIMPLY CANNOT FLIP FLOP BACK AND FORTH BETWEEN THE TWO POSSIBLE POSITIONS. MUDDLING THROUGH WILL SIMPLY GO NOWHERE.
-
CHAPIN

**Fig. 10** Excerpted Declassified State Department Cable From Amb. Frederic L. Chapin to U.S. Secretary of State George Shultz, Urging Taking a Moral High Ground on Guatemala. Source: The National Security Archive The Guatemala Project

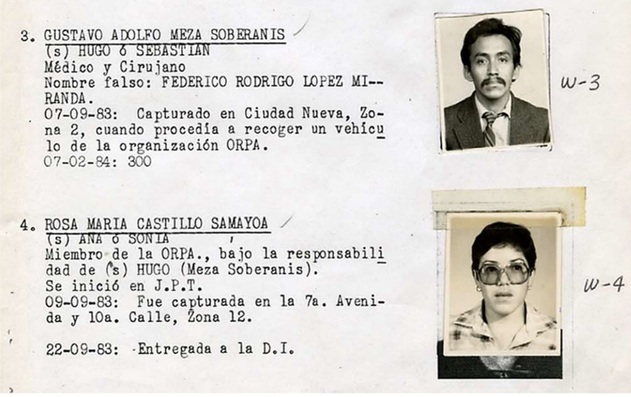
[34] Deputy Chief of U.S. Embassies (Missions) is that party who is second-in-command to the Ambassador - credentialed to the/any State in concern

[35] Staff serve as independent policy analysts and key advisors for the U.S. Secretary of State, who is the Principal Diplomatic Officer of the United States, and a Cabinet Secretary (Cabinet Minister equivalent)

*assistance ha[d] not been so much in terms of arms sales, but in what [was] loosely [to] be called "services," i.e., various forms of cooperation and use of advisors."* [80] Bahbah and Butler also documented that during that time, with Israel's assistance, Guatemala's *"military government subdued its guerrilla challenge and…the government attribute[d] the success of its efforts in this regard to the lack of U.S. oversight and advice, [that] enable[ed] it to find its "own solutions." Such solutions-widely agreed to have been unparalleled in violence-included scorched earth campaigns, the bombing, burning and bulldozing of entire villages, massacres in the countryside, and death squad killings in the city"* [81].

Israel was fully aware of the repressive history of the Guatemalan Government. Yet, Israel's defense establishment supported by the central government, was eager to do business in Central America. Yohanah Ramati, a former member of the Israeli Foreign Relations Committee during the 1977–1984 'Likud' government, branded Israel's willingness to work unscrupulously with anyone in the world, in the following fashion. Of Israeli policies regarding the matter, Ramati observed, *"Israel is a pariah state. When people ask us for something, we cannot afford to ask questions about ideology. The only type of regime that Israel would not aid would be one that is anti-American. Also, if we can aid a country that it may be inconvenient for the [U.S.] to help, we would be cutting off our nose to spite our face not to"* [82].

As a side note, Bahbah and Butler assert in their writings that Israel had an unbridled willingness to do business with unsavory regimes in Central America. They wrote, that in such dealings, Israel chose to *"impose no restrictions for reasons of moral and political distaste (e.g., human rights)," and that "Israel supplying the anti-Semitic military junta of Argentina in the 1970s and early 1980s [represented] one of the more unsavory…"* [83] example of such relationships. Additionally, while a UN embargo was in place, violating it, the Israelis armed Bosnian forces who then perpetrated massacres; it supplied arms to Chile and Nicaragua and more recently to the evildoers in South Sudan [84]. Israel's cooperative arrangement with the then oppressive Guatemalan Government served to entangle its whole population in a web of surveillance (as it will be seen below), and to immerse Guatemalans into a generation or more of bloodshed. Figure 11.



3. GUSTAVO ADOLFO MEZA SOBERANIS
(s) HUGO ó SEBASTIAN
Médico y Cirujano
Nombre falso: FEDERICO RODRIGO LOPEZ MI--
RANDA.
07-09-83: Capturado en Ciudad Nueva, Zo-
na 2, cuando procedía a recoger un vehícu
lo de la organización ORPA.
07-02-84: 300

W-3

4. ROSA MARIA CASTILLO SAMAYOA
(s) ANA ó SONIA
Miembro de la ORPA., bajo la responsabili
dad de (s) HUGO (Meza Soberanis).
Se inició en J.P.T.
09-09-83: Fue capturada en la 7a. Aveni-
da y 10a. Calle, Zona 12.
22-09-83: Entregada a la D.I.

W-4

**Fig. 11** Dossiers of Two Victims of Guatemalan Death Squads, Surveilled and Tagged. Source: National Security Archive - The Guatemalan Project

> "The bureaucratic procedures for approving the killing of a dissident are well-established. "A local military commander has someone they think is a problem," the officer explains. "So they speak with G-2, and G-2 consults its own archives and information from its agents and the police and, if all coincide, it passes along a direct proposition to the minister of defense. They say, 'We have analyzed the case of such and such a person in depth and this person is responsible for the following acts and we recommend that we execute them.'" …"Prominent Political dissidents get special consideration. "When there is a big fish, G-2 makes a presentation, they review all the problems with the person, the objective of the mission, and their recommendation. They can give three options—disappear [kidnap and execute] them, eliminate them in public, or simply invite them to leave the country." [85]

Around 1979, An Israeli defense industry firm Tadiran, installed information technology service tools for the notorious and ruthless Guatemalan Police Intelligence unit, the G-2. The G-2 systematically amassed electronic dossiers on all those who were considered sympathizers, collaborators, aiding and abetting voices, actors in, or supporters of governmental opposition, such as those that were suppliers, transporters, facilitators/brokers; any and all.

On one hand, the electronic dossiers served to identify specific Guatemalan persons for execution. On the other hand, the information technology and the surveillance network to which it was connected served to identify 'out of the ordinary' use of utilities (water, electricity etc.) by those among the population who could be anti-government radical operatives [86]. Subsequent to the information technology installation in Guatemala with the assistance of Israeli Intelligence (who, according to Jane Hunter, *"text-booked the operation"* in-line with Israel's *"experiences in Palestinian areas"*), the Guatemalan Government began the registration of the entire population in 1983. By 1985, Guatemala had registered 80% of all adults in their population [87]. In El Salvador, the same equipment was supplied by Tadiran to catalog people there.

The world began to see the possibility of the 35 + year civil war in Guatemala coming to an end, as steps toward peace were formally underway in 1996, when under the auspices of the United Nations, Government of President Alvaro Arzu Irigoyen signed Peace Accords with rivalling factions in the country, with optimism of restoring peace and tranquility through a reconciliation process.

For the purposes of this Editorial Chapter and more direct Privacy and Security considerations, it is vital to be reminded that in the instance of Guatemala, the people of Guatemala, through its government was a signatory to the Universal Declaration of Human Rights in 1948. In that regard, the following conclusions, which the United Nations sanctioned "Commission for Historical Clarification" (Guatemala) arrived at, will be important to reference herein. The Commission concluded that the killings, the genocide in Guatemala over **35** years amounted to be *"grave violations of international human rights law whose precepts the Guatemalan State ha[d] been committed to respect since it approved the Universal Declaration of Human Rights and the American Declaration of the Rights and Obligations of Man in 1948"* [88].

Moreover, the Commission explicated that *"[a]s regards international humanitarian law, which contains the obligatory rules for all armed conflicts (including non-international armed conflicts), the [Commission] concludes that Guatemalan State agents, the majority of whom were members of the Army, flagrantly committed acts prohibited by Common Article III of the 1949 Geneva Conventions, particularly with respect to attacks against life and bodily integrity, mutilation, cruel treatment, torture and torment, the taking of hostages, attacks on personal dignity, and particularly humiliating and degrading treatment, including the rape of women," and "that many massacres and other human rights violations committed against […] groups obeyed a higher, strategically planned policy, manifested in actions which had a logical and coherent sequence"* [89]. The Commission placed the blame squarely upon governmental structures and parties within them, for driving and the administrating of horrific crimes in Guatemala, declaring, *"the State of Guatemala holds undeniable responsibility for human rights violations and infringements of international humanitarian law"* [90].

Realization of Privacy and Security as basic values in a modern society, in the Digital Century, will ultimately be the byproduct of having a "civil" society, where a "civilizing" of humankind has permeated to each individual in society, and a 'high-bar' has been set in relation to Privacy and Security as 'must-have' values, where persons will be, and are, held accountable for transgressions and outright criminalities done against 'high-bar' values. Instead, what we have is the following. From such long-lasting civil-wars as in the case of Guatemala and El-Salvador, violent elements, and indeed, a culture of "total violence" and all its components have since transcended Salvadorian and Guatemalan borders, and has rooted itself around the world in the form of a gang termed as 'most ruthless,' the **'Mara Salvatrucha'** or **MS-13**. As this Editorial Chapter was being written, gang and political violence of a close-contact nature is once again claiming *"wrong-place at the wrong-time"* innocents in Guatemala. Corruption is running rampant. No respect for anyone's Privacy, Safety, or Security can be expected in such volatile and corrosive environments. Lastly, beyond political, social, military, and economic entanglements, lay a more foundational entanglement – of a moral nature. *Beyond arming unsavory regimes, facilitating torture and murder, and clandestinely looking the other way, is that moral entanglement, where, "one hopes forever," that none will lay blame for the more foundational moral lapses made.*

Consider that the United States signed the Universal Declaration of Human Rights, as did Guatemala, and as did Israel. Yet, more foundationally, the Declaration was violated, and substantive acts (some of which are detailed here) by all involved, assisted to careen an entire ancient civilization toward a modern moral and ethical abyss. Reminding Israelis that the Jewish State had ratified the Universal Declaration of Human Rights, and that the Declaration itself *"was drafted in the shadow of the Holocaust horrors and in view of millions of homeless refugees,"* a Israeli Newspaper had warned its readers in 2011, that by nature of Israel's involvements and specific activities, the State was now jeopardizing the very existence of human rights in Israeli society [91]. More recently, the same newspaper through an Editorial, told its readers to be aware that their nation was arming the repressive Government in Myanmar [92], acknowledged by the international community as conducting violent ethnic cleansing actions against the Rohingya, a minority population.

Throughout, the author has made attempts to demonstrate that a mere presence of laws in society is grossly insufficient, while pursuing to lay esteem to Privacy and Security as prime values in society, and detailing of the need for a watchful eye, and invigorated actions toward sustaining Privacy and Security values over time. As an example, among other essentials components that must exist in the mix would include law enforcers who have good training - in the full range of their duties and a clear comprehension of the range of laws they must enforce. They must have appreciation and respect for law and order, borne out of a personal understanding of civility and Constitutionality, and must have demonstrated their ability to be moral and ethical in their actions. [93] Most of all, the central message within this section has been that Society, and those who are in it, must be civilized. Without a very individual "civilization," the possibility to uphold and/or express "human rights" meaningfully, at any level will be questionable. All along, we must also ask, what becomes of the Privacy and Security of citizens in a State, when vast instrumentations of the State are organized against its citizens? What is to be the result of a foundational deterioration, or corruption in the way a State is organized; intellectually, legally, or say, morally?

## 4 Re-establishing human rights foundations in the long shadow of atrocities - the Rwandan experience

There are particularly good reasons as to why this Journal's Special Issue on Privacy has featured within it, key contributors from the Republic of Rwanda, and the Republic of India. Before exploring those reasons and examining the cases of Rwanda and India, the author wishes to petition the reader to ponder the extent to which our Personal Privacy and Security standards have become developed, and have, or have not become expressible, in terms of the Universal Declaration of Human Rights (UDHR) is a reflection of how civilized we have become as a society. The aforementioned matter of "civilizing" will at least be peripherally discussed, and to the extent possible, within the scope of this editorial in order to demonstrate the basis for that assertion. Figure 12.

More generally, we must take note that, *the travesty that humanity as a whole must now unambiguously and totally confront is the verity that the human race cannot logically lay claim to be civilized, to be 'improved,' whilst being incapable of expressing through actions, the very essence of 'a civilizing' to which we lay claim.* Respect for human life is paramount in terms of the Universal Declaration of Human Rights; and Privacy is a sub-set of the UDHR. Examination of current conditions within the Republic of Rwanda, and the Republic of India - in the overall – amount to teachable moments for the human race, in relation to Personal Privacy and Security.

Rwanda today is a nation that offers nearly universal health care for its citizens, and 12 years of public schooling for all children, and as a Republic with limited resources, they have managed either to meet, or to exceed the United Nations' Millennium Development Goals.[36] The nation has managed to successfully halve for instance, "the proportion of people suffering from hunger, and has made good progress toward reducing by half, the proportion of people living below the national poverty line and those living in extreme poverty."[37] Rwanda today is a rising economic force on the Continent of Africa, and among one of the fastest growing Sub-Saharan, and African economies in the overall [94], while Kigali, the Capital City is considered the cleanest and safest on the Continent. Perhaps none of these achievements will have been possible, if the Republic and her people had not made the decision, and to thereafter be determined to follow-through on national commitments to repair and heal from the horrors of the past; to rise from the ashes.

**Fig. 12** President Paul Kagame of Rwanda gesturing at "The Transformation of Tomorrow" Session at the annual meeting of the World Economic Forum in Davos, Switzerland, Jan. 20, 2016. Courtesy of: Reuters/Ruben Sprich

From that nation's colonial histories, to the genocide against the Tutsi, in 1994, Rwanda has had to bootstrap new beginnings from the stampings of a failed state. Rwanda has had to re-invent itself from a state where many instruments of central government had once organized, and had aided, in the cordoning of citizens for massacre among other things, to the challenge now of having to drag an agrarian population along [95] into a democratized future with newly established constitutional foundations and all other relevant instrumentations of a modern society. Such an effort is not something that an unprepared mind can sufficiently comprehend, not only due to the level of social and economic complexities involved, but due to the level of governmental discipline, and also the sheer level of sharp and determined focus that needs expending toward re-institutionalizing a type of focus that is constantly and consistently required for transformative purposes.

In these highly troubled times, Rwandan Government's participation in the Special Issue represents great personal courage on the part of the particular participant personally, and is additionally a sign of a promising direction for people and those instruments of national governance.

At the 2015 and 2016, World Economic Forum (WEF) meetings in Davos, President Paul Kagame was visibly engaged in informing and educating WEF attendees that Rwanda was committed to be a forward-thinking and forward-looking country, with many strategic initiatives underway - to rapidly transform the nation. During the meeting, President Kagame urged participants to consider the Economic promise of Rwanda, and that within the

[36] Translated to apply locally as Economic Development and Poverty Reduction Strategies (EDPRS) I & II

[37] Millennium Development Goals Monitor (MDGMONITOR) http://www.mdgmonitor.org/

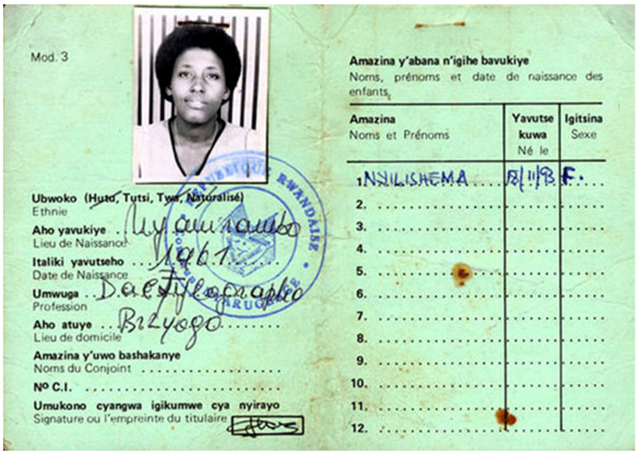
Continent of Africa as a whole. In hearing the President's perspectives and appeals, the author was starkly confronted with the high-contradictions, and the several devils that Kagame had to have been battling – even before he got out of bed that morning for the WEF meeting in Davos, on 20 January 2016.

On one front, Kagame and his administration were clashing [96] with entrenched accusations of political repression, muzzling of the press, and criticism, extrajudicial killings, and authoritarianism among others [97]. On another front, Kagame had arrived in Davos, intent on gaining international support and commitment for his social and economic visions [98], one that entailed the transformation of a struggling small African nation with its agrarian economy into an Information and Communications Technology (ICT) driven powerhouse on the African Continent. On yet another front still, Kagame, who is largely recognized as having been[38] responsible for ending the large-scale massacre of civilians in 1994, has had to look beyond his nations past, in order to lay the first cornerstones for a new Rwanda, to be built upon blood-soaked soils.

Listening to President Kagame at the time, this author had concluded, and perhaps not unlike other political scientists [99] that, in all manner of activities endeavored and accomplishments achieved by Rwanda would likely be viewed by the world through the lenses of the "ghosts of horrors past," and that the use of those lenses would perhaps be unavoidable, given the nature of the horrors that transpired. Yet, there was a sense of hope, vitality, and conviction in President Kagame's message, which he presented in Davos, on behalf of his people.

The challenge that ran through this author's mind at the time was, how it will be possible for the world to assist the Rwandan people advance, in relation to ICT, and in relation to Privacy and Security, and still ensure that the horrors of the past have fewer than any chances at all to revisit [100]. *This was particularly important going forward since core to Rwanda's plans to transform its national economy involved thoroughly modernizing the nation's internal ICT capacities and capabilities.*

Given the tragic history of the Rwandan genocide against the Tutsi, in 1994, where: 1) government issued national ID cards with ethnic identifiers (See Fig. 13) facilitated the mass killing Rwandan citizens, and 2) where the government had once organized itself and aided in the killing of civilians, the present day government's commitment to creating large-scale national operational efficiencies and sufficiencies based on ICT modernization could be very troublesome, if the improved ICT infrastructure, various components, and functionaries were to fall into the wrong hands at any point in the future. *The view, with respect to Rwanda's running initiatives to modernize, imposed a larger consideration, that with specialized ICT infrastructure, facilities, operational modalities, capacities, and developed capabilities, and the scope of proposed Rwanda ICT penetration into government and civil sectors could enable an iniquitous future government, where it's proscribed arms or agents, could once again bring evil acts upon innocents.*



Mod. 3

Ubwoko (~~Hutu~~, Tutsi, ~~Twa~~, ~~Naturalisé~~)
Ethnie

Aho yavukiye .. Nyamirambo
Lieu de Naissance

Italiki yavutseho .. 1961 ....
Date de Naissance

Umwuga .. Dactylographe
Profession

Aho atuye .. Biryogo .......
Lieu de domicile

Amazina y'uwo bashakanye
Noms du Conjoint ..................

Nº C.I. ..........................

Umukono cyangwa igikumwe cya nyirayo
Signature ou l'empreinte du titulaire

REPUBLIQUE RWANDAISE

Amazina y'abana n'igihe bavukiye
Noms, prénoms et date de naissance des enfants

| Amazina<br>Noms et Prénoms | Yavutse kuwa<br>Né le | Igitsina<br>Sexe |
|---|---|---|
| 1. NYILISHEMA | 18/11/93 | F. |
| 2. | | |
| 3. | | |
| 4. | | |
| 5. | | |
| 6. | | |
| 7. | | |
| 8. | | |
| 9. | | |
| 10. | | |
| 11. | | |
| 12. | | |

**Fig. 13** Rwanda National Identity Card circa 1994 - Identifying a National by Race, a Tutsi. Source: Genocide Archive of Rwanda - Aegis Trust, Kigali, Rwanda, 2017

Fittingly, subsequent to the WEF meeting, this author sought cooperation from the Government of Rwanda to ink for the Special Issue, a contribution that would highlight the transformative efforts being undertaken by the Rwandan Government, shedding light on corresponding lawful and constitutionally protective measures that the government has been planning and implementing in relation to ICT modernization, for the sake of the Rwandan population. The intention was to have the Rwandan Government indicate to the scientific and policy communities, the ways and means through which the Rwandan Government had planned to protect and safeguard the life and limb of present and future citizens of Rwanda from malevolent ICT use, regardless of persons in power.

Following consultations, His Excellency Jean Philbert Nsengimana, Rwanda's Cabinet Minister for ICT, tendered a composition reflecting Rwandan Government efforts to protect the Privacy, Safety and Security of Rwandan citizens and residents, given the Republic's strategic ICT initiatives and plans. Minister Nsengimana's contributions will undoubtedly stand as a small testament to not only his personal courage, but also to the government's desire to share with the world, their commitment to instituting ongoing robust measures of national unification, reconciliation, reconstitution and the establishment of protections for citizens and residents of Rwanda from the perils of ICT

[38] As Commanding General of the Rwandan Patriotic Front (RPF) Army

use. The author has been advised that the nation's strategic ICT plans are based upon a leadership vision to have Rwandan national revitalization and ICT modernization efforts co-exist with the evolution of governmental channels and processes - undertaken to establish systems and laws to assure data safety and protections for all within its national boundary. His Excellency, Minister Nsengimana's contribution to the Special Issue details [101] much of these efforts.

## 5 The case of privacy in India

Privacy and Security evolution in the case of the Republic of India should afford each of us distinct opportunities to discover world-fissures that prompt a questioning of our individual constitutions in relation to the world in which we live, chiefly tagged these days (wrongly) as being *"too complex or too violent and crazy to deserve serious reflection"* [102]. Narcissism, isolation, racism, xenophobia, extremism/nationalism, fanaticism (religious, political, economic, militaristic), and authoritarianism/fascism are indeed on the rise the world over, but, there must be push-back; for within improving societies, such sociopathies must be reversed through intensified vigilance at the individual level, very sensitive public awareness, education and the intellectual transformation of every member in our society. After our total examination of Privacy and Security states here, founding a 'reconciliation' process in the context of a larger need to establish civil societies might be a good beginning. However, before we can inch toward any 'Reconciliation' process, even symbolically, each of us collectively must examine those things that are preventing us from categorically understanding the true depth and the scope of the intellectual misunderstandings related to Personal Privacy and Security in relation to the world we inhabit. Figure 14.

At the present, Privacy and Security inconsistencies are outgrowths of society's incorrect focus and posture - only upon those concerns involving misconfiguration(s) in/of, instruments of law and/or their foundations. This is not where our attention should be solely. Societal weaknesses to establish, and durably maintain Personal Privacy and Personal Security keystones are more a function of how society is not organized (or is largely unorganized), and has been inadaptive to rapidly occurring globally interconnected changes. Observing and being students of occurrences and experiences emerging in the Republic of India will likely hand to each of us greater clarity and the motivation to elevate Personal Privacy and Security appreciably to needed levels where the global struggle to meet and exceed knowledge economy related challenges can be fulfilled without compromising ourselves any more.

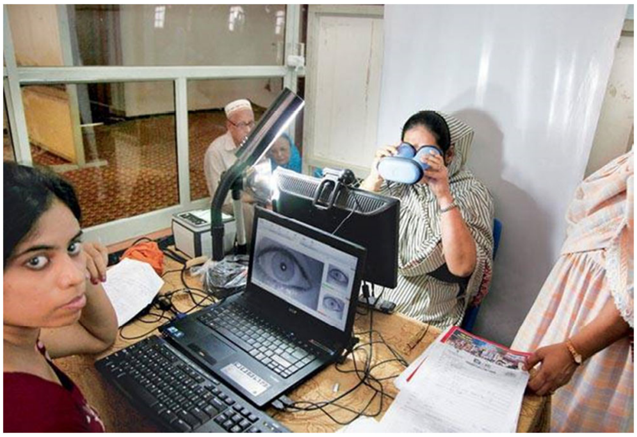


**Fig. 14** Registering Participants in the *Aadhaar* The World's Largest Biometric Identification Program (India) Courtesy: Reuters

### 5.1 Privacy ruling in India: one small step for man – one giant leap for mankind, or is it?

On 24 August 2017, with the words, *"[l]et the right of privacy, an inherent right, be unequivocally a fundamental right… [t]his is the call of today. The old order changeth yielding place to new,"* [103] the highest court in that Republic, ruled that Privacy was a fundamental right for nearly 1.4 billion of the world's human beings. To an onlooker, however, the Privacy situations and the plethora of Human Rights issues that the Indian people are wrestling with, presents enormously perplexing and deeply conflicting pictures.

On one hand, preceding the Supreme Court ruling, the Government of India under the leadership of Prime Minister Narendra Modi had unconstitutionally been fully committed to, and was in the middle of, administering to every Indian citizen, an officiated permanent digital implant that w/could permit routine and persistent surveillance of the whole population.[39] On the other hand, the Indian Supreme Court ruling has philosophically reversed the natural poles of the planet, for no court of any kind, anywhere has ever affirmed, and done so concretely, that Privacy was someone's elemental right. Not only was this ruling, one of an inter-stellar proportion for humanity everywhere, but, the Supreme Court essentially sowed the seeds to apply the brake, even to arrest - all personally intrusive measures that the Government of India had undertaken to that date, and that the Government was fully intentioned to have continue. Despite the Supreme Court ruling, the Indian Government still actively maintains efforts throughout the country to register Indian citizens into its Biometric ID program called the *Aadhaar*, considered

[39] The *Aadhaar*, India's Biometric ID Program will be discussed very briefly later in this section

the largest in the world, which (when, and if completed) will have registered and tagged nearly 1.4 billion people.

How was it possible for the Indian Government to implement a largely unconstitutional program among 1.4 billion people, in *"the world's largest democracy,"* and by a machined legislative decree? Better still, how exactly did India swiftly get onto the surveillance super-highway? Such are the questions that should be asked, and some of them will be explored further in this section, giving sufficient granularity into India's current experiences, also with due considerations to that long-lived land, her rich and celebrated history and her wise peoples.

Given India's 4000+ year history, if anything, she should, by all accounts be one of the most advanced Republics on the planet, with firm foundations, principles, practices and practitioner wisdom to pass on to the rest of the world not only in the area of Privacy but, in all matters related to Human Rights. However, in every such respect, in the present days, the Republic of India is a nothing short of a conundrum. This author has determined that there exists a critical necessity to discuss a number of key areas related to India, and her history, which will be relevant to any broader discussion on Personal Privacy and Security, worldwide.

As a Parliamentarian, the Honourable Tathagata Satpathy from the Republic of India has accustomed us in *"The Aadhaar: "Evil" Embodied as Law,"* [104] that India is known the world over for many things; the origin of human languages, grammar, literature, music, medicine, mathematics, physical sciences, art, etc. In a matter quite directly related to the 'civilizing of the human race' more broadly, the following aspect related to India's history must surely be considered, for it is a matter that contributors discussing dilemmas now faced by Indian people have not covered. Those discussion points are highly relevant historically, and contextually, in terms of all considerations related to the establishment and maintenance of Personal Privacy and Security environments everywhere..[40]

## 5.2 "World's largest democracy" and a glimpse into India's privacy related human rights conflictions

*"The Greeks before the time of Pythogoras, travelled to India for Instruction. The signs of the seven planets and of the seven metals are still almost all over the earth, such as the Indians invented. The Arabians were obliged to adopt their cyphers. Those of games, which do the greatest honor to the human understanding, incontestibly come from India; as elephants, for which we have substituted towers, evince. In fine, the people who were the earliest known, the Persians, Phenicians, Arabians, Egyptians, went from time immemorial to traffic in India, in order to bring home spices, which nature has given to those climates alone; but Indians never went to ask any thing from other nations,"* said Voltaire [105].

Eventhough India's history (some of which is obscure), is vast and rich, the untrained Western mind is tuned to receive only chronological signals of History since Indian independence in 1947. It is for this reason that a delving into India's early periods must be performed to better contextualize discussions related to Personal Privacy and Security.

Despite colonial and post-colonial efforts to blur historical chronologies [106], India, is arguably the seat of the world's oldest [107] Republic [108], which also gifted to the world, the *Arthashastra* [109], the ancient world's tome on matters of statecraft, and the administration of Empire. The *Arthashastra* [110], was antiquity's manual of polity and governance; on establishing and maintaining accountability, details related to economics, finance, manufacturing, trade, commerce, laws, punishment, strategic actions for Empire/Nation etc., written by the Indian philosopher, visionary statesman, and political economist Chanakya/Kautilya (350–275 BCE). The *Arthashastra* [111], was in essence, part of a framework created for an Empire to establish and maintain social order, economic and military superiority, peace, sovereign borders, and a guide to the maintenance of individual moral qualities and expected societal behaviors.

In full view of modern-day Nation State mass surveillance activities, studying that which Philosopher/Teacher/Kingmaker Chanakya had once inscribed in *Arthashastra* [112], will be important to consider, especially since the text amplifies the need for good government and good governance, among other things. One example of good guidance from Chanakya is, where he said, *"[i]n the happiness of his subjects lies his [the King's] happiness; in their welfare his welfare; whatever pleases himself he shall not consider as good, but whatever pleases his subjects he shall consider as good."* In the land of the *Arthashastra* then, how could the central government foist upon the Indian population, anything that could have become a source of great malady to the public's welfare?

Algernon Sidney once compelled us to comprehend that *"if governments arise from the consent of men, and are instituted by men according to their own inclinations, they did therein seek their own good; for the will is ever drawn by some real good, or the appearance of it. This is that which man seeks by*

[40] *"...to condemn the past, as full of error and delusion, and then to set forth what we imagine to be our own fundamentally significant and wholly new methods in philosophy, is a procedure that in general can have but one ending. We, then, but unwittingly transplant old growths to new soil, seeing not how old the growths are, and considering only the newness of the garden that we have planned. But the new soil is of necessity lacking in the ancient wealth and depth, and the transplanted doctrines take little root."* – Royce, Josiah; "The Spirit of Modern Philosophy: An Essay In The Form of Lectures," Houghton Mifflin Company, Boston, USA 1892

*all the regular or irregular motions of his mind. Reason and passion, virtue and vice, do herein concur, tho' they differ fastly in the objects in which each of them thinks this good could consist. A people therefore that sets up kings, dictators, consuls, pretors or emperors, does it not, that they may be great, glorious, rich or happy, but that it may be well with themselves and their posterity"* [113]. So, did Indians knowingly direct their government representatives to decide unpropitiously in the matter of the *Aadhaar* legislation, which was destined to inflict upon the people, a treacherous and problematic posterity, or were they somehow fooled into electoral action? If the Indian people were fooled, how could such distress and misfortune arise, given their age-old experience with governance, and in many flavors? On the other side, the side of those elected Indian government representatives, did they forget that *"[g]overnment is not instituted for the good of the governor, but, of the governed; and power is not an advantage, but a burden"?* [114]

### 5.3 Is India an Ochlocracy [115], and what are the privacy and security implications?

India's Constitutional Preamble states: "WE, THE PEOPLE OF INDIA, having solemnly resolved to constitute India into a [SOVEREIGN SOCIALIST SECULAR DEMOCRATIC REPUBLIC]."[41] Why is an analysis of the Indian governmental orientation and organization of importance to a Privacy and Security discussion? If the task of protecting Personal Privacy, and ensuring the Security of citizen information is to fall to the government, to what extent, and how well, will the Government be able to perform those functions? Stated in another way, the manner in which the government is organized, its many instruments are aligned or misaligned (to facilitate governance), its laws, how government administers etc., is all functionally important to how well Privacy and Security as desired values are, or can be, protected and cherished. In this vein, constitutionally established descriptions and authorities are very important for the purpose of daily operations; but, by no means should a national constitution be considered a limiter, for constitutions can be modified to fit changing needs over time. Nevertheless, it is a guidepost to present-day thought, and accompanying instrumentations to be in place to facilitate governance. Therefore, when constitutional elements present foundational confusion, there are bound to be structural problems integrally, that follow. Briefly then, the following points are noted to give the reader an appreciation of the seriousness, intricacy and the range of the problem set. Terms like "Democracy," "Republic" and "Socialism" remain all-too confusing for the layman, and have remained so. If the United States is to be used as an example to illustrate the point, and it should (as a more mature modern Republic in comparison to India), the following points are extremely important contextually, to the establishment of Privacy and Security protections, maintaining reliability structures and originating citizen benefits that are now constitutionally protected in India.

As an example, let us examine the term "Democracy," for the prevailing confusion the term generally announces. Concentrating on the United States as an example, many 'Founding Fathers' of the nation loathed the notion of an enshrined "Democracy." The antipathy that John Adams had for "Democracy" is made obvious to us - in this time – by reading Adams' letter to John Taylor, wherein he says, *"Democracy never lasts long. It soon wastes, exhausts and murders itself. There never was a Democracy yet, that did not commit suicide"* [116].President George Washington communicated similar feelings of revulsion as Adams, so noted the first, and the most venerated Chief Justice of the United States Supreme Court, John Marshall, in his writings on the life and times of Washington. Marshall penned, that Washington was of the belief that, *"[b]etween a balanced republic [representative structure] and a democracy [rule by the people], the difference is like that between order and chaos"* [117].

The United States is structurally not a "Democracy." Still, the "Democracy" fallacy runs deep and wide, especially among many mandarins (elected representatives, political appointees, department and agency heads etc. etc.) of the day in U.S. government, who neither understand the function of government, nor the precise manner through which government functions are to be carried out for the benefit of the people to meet constitutional sufficiencies [118]. In "Democracy Not the Crowd: Our Popular Delusion," political theorist and philosopher Mary Follett wrote*"[when] we define democracy as the "rule of the whole," this is usually understood as the rule of all, and unless we fully understand the meaning of "all," we run the danger of falling a victim to the crowd fallacy. The reaction to our long years of particularism, of "individual rights" and "liberty," which led to special privilege and all the evils in its tram, has brought many to the worship of the crowd"* [119].

While what is about to be said, should not be interpreted as a book review, in agreeably more plain language for the non-social science person, that philologist, the political scientist, political economist, public administration scientist, or students of political constitutions and political

[41] The Constitution of The Republic of India – "This information is downloaded from the website of Ministry of Law and Justice (Legislative Department)" 9 November, 2015 http://lawmin.nic.in/olwing/coi/coi-english/coi-4March2016.pdf [notes related to amendments within the cited portion of the Preamble, are not included] AND National Portal of India at: https://india.gov.in/my-government/constitution-india (more user friendly)

constitutionalism, Viscount Richard Haldane once encouraged a reading of Follett's astute awareness, and acumen on Democracy. Of her writing, Viscount Haldane said, *"[i]t is the exposition of a principle which is not stated for the first time, but which, in the form and connection in which she states it, seems to place many difficulties in a new light, and to lay to rest controversies, some at least of which have arisen out of misinterpretation of what is fundamental"* [120]. Haldane's perception related to "Democracy" related misinterpretations as noted by Follett (and others), persists today, and is more common. The unmistakable spreading of "Democracy" falsehoods by pseudo-intellectuals, is at least partially responsible for government mal-orchestration and inoperability, and uninteroperability. Philosopher of History, Cornelius Castoriadis has written much about this [121]. That said, a layman could potentially comprehend the terms, "Sovereign Republic" and a "Secular Republic." But, what clearly is a "Democratic Republic," or a "Sovereign Socialist Secular Democratic Republic," given the problems that lay-people have with "Democracy" as a word?

Wisdom on government and governance from Chanakya, the martyred Whig Algernon Sidney, John Adams, Marshall, and Washington aside, the contemporary frame of reference for considerations and discussion on Personal Privacy and Security is the Universal Declaration of Human Rights of 1948.[42] The most interesting aspect of the Universal Declaration of Human Rights, beyond the declaration itself is the fact that this document broke the world record for being the most translated document in the world, in 1999, at 370 languages and dialects [122]. Today, there are over 500 distinct translations available. Quite obviously, the world is eager to have this document and the message it contains; the world must feel a great kinship with the value of the message within. Relationally, it is worth observing that in *Arthashastra*, Chanakya had captured the quintessence of UDHR as indispensable cornerstones to advancing just, peaceful and thriving societies. Chanakya had inscribed that, *"[h]armlessness, truthfulness, purity, freedom from spite, abstinence from cruelty, and forgiveness are duties common to all." .... "For the world, when maintained in accordance with injunctions… will surely progress, but never perish."*[43] This is the backdrop against which, we must consider the challenges that Indian society is/will be facing, and considering further, just what, and how, we can learn from these ongoing Indian experiences, to restructure and modernize international safety and security frameworks.

**Fig. 15** Hindu nationalist summer camps for girls take place across India, all operated by an organisation called the Durga Vahini. (In: "India's Hindu Fundamentalists). Courtesy: Al Jazeera

## 5.4 Forward political climate

The first component to consider is the current political climate in India. Former Reserve Bank of India[44] Chairman and academic, Raghuram Rajan, took the opportunity to illustrate, what India will have to look forward to, if India continued down a path of political disorder, and if institutionalized corruption continues to advance unabatedly. Rajan diplomatically admonished the mandarins, saying, *"[b]y killing transparency and competition, …[a]nd by substituting special interests for the public interest, it is harmful to democratic expression"* [123]. Curbing of one's freedom of expression hurts a Republic. Privacy and Security of personal information related insecurities fall under actions of States to curb personal freedoms, such as expression.

Corruption is a front-runner in a list of maladies that plague the Indian republic, and its very existence. Corruption at every level of society has threatened individual freedoms in India for decades; and now, its continuation, aided by ideologies and the machinery of political extremism rearing prominence (See Fig. 15) in the Digital Century - makes India's very existence, and the vibrant potential of every individual resident in India, at threat. Extremism/Tribalism and corruption has had a long co-existence in the Indian society. The effectiveness and performance of Privacy and Security protective foundations in law, and all other means of remediation will for example, be ultimately hinged to the government's ability to work past 'hard-entrenched' corrupt functionaries and their instruments, which are completely unreliable. Interestingly, one World Bank research report had characterized the nature of country's corruption as, *"widespread,"* and that *"…corruption within India's legal system and government significantly weakens legal protection in practice"* [124].

Recently, Milan Vaishnav of the Carnegie Endowment for International Peace wrote from his research that *"it is clear that criminality in politics [in India] is widespread"* and that *"candidates linked to crime appear to have a hefty electoral*

[42] India was one of the original signatories to the UDHR

[43] Chapter III, "Determination of the place of the Triple Vedas" among Sciences in Book I, "Concerning Discipline" - The Arthasástra of Kautilya

[44] The Central Bank of India

*advantage"* [125] In reference to the same topic, Vaishnav noted, and more importantly that, *"a candidate with a criminal case was, on average, almost three times as likely to win election as a candidate who faced no cases"* [126]. This is the living and breathing political constitution and governmental environment within which Personal Privacy and Security must find it possible to land, survive, and thrive. Consequently, a sensible individual is forced to ask if India, and her nearly 1.4 billion people are part of a *Republic*, or an *Ochlocracy* [127]. The author herein shall aim to make note of a limited number of examples that will support the need to have that question answered, and properly, without evasion. There are many reasons to why such questions are eminently pertinent, in terms of Personal Privacy and Security.

Political stability, and the economic future of India (at the least - as a regional power) in the Digital Century are of great concern to many external to India, apart from those within. The need for concern and pause emanates from the understanding had, that, *"[w]ith weak government administration at the federal and state levels, poor intelligence, and growing corruption, criminal elements have gained opportunities in India's political system, and criminal-state and criminal-communal nexuses have emerged"* [128].

The new Prime Minister was elected making uncompromising promises (at least superficially) declaring that he would, and could, tackle the rampant corruption in the country [129], where **70%** of the population now pays a bribe to obtain the most basic of services [130]. In terms of discussing how effectively Human Rights (of which Personal Privacy and Security are components), or the UDHR are, and will be honored, extended, and preserved in the Indian society, a short discussion of key societal aspects foundationally essential to buoying and defending of the "Indian democracy" (such as it is), and of the upholding of key principles will be prerequisite.

Narendra Modi was sworn in as the **15th** Prime-Minister of the Republic of India, in May of 2014 upon the back of a rising Hinduistic-extremist tide. Prior to Modi's ascension into the role as the new Prime Minister of the Republic, he had been banned from entry into the United States, since 2005, for his political role in not curbing religious riots, and particularly in not preventing the loss of life in said religious riots. Modi has been the only political entity to be banned entry into the United States, for: as the United States Department of State put it, *"any foreign government official who "was responsible for, or directly carried out, at any time, particularly severe violations of religious freedom" [is] ineligible for a visa to the United States"* [131]. Hindu nationalism is on the rise in India, and as never before in recent memory, and in part, Modi's win has surely given rise to the same. A member of the *"Rashtriya Swayamsevak Sangh"* (RSS), a Hindu nationalist organization since childhood, Modi rose through Party ranks, artfully constructing the party message along the way, communizing and popularizing the notion of creating a new India; a Hindu nation, with a dominant Hindu ideology; shunning pluralism and secularism. Since his installation, Modi has promoted his ideas for a new India, as in the case of rejecting secularism (in line with RSS political orientations), and encourage and even endorse India-wide cretinism through *"Saffronization,"* a process of causing adhesion to revisionist histories by way of creating select textbooks [132] and machining an educational curricula suited for such a purpose [133].

Despite persistent accounts (among other things) of "Hindu-Muslim" conflict, India's history has seen secularism finding a reasoned and near dominant place in society, especially since the Mauryan Emperor Ashoka, in 270 BCE. It is not a minor point, nor is it an accident, that Ashoka promoted secularism as a core ideal for his Empire and encouraged its thriving beyond, for Ashoka was the grandson of Emperor Chandragupta Maurya, whose was tutored and advised by Chanakya.

Also not a minor point is the fact that Prime Minister Modi, since his inauguration has, carefully engaged in the entrenchment and proliferation of nationalistic ideology by disquieting means. Carefully massaged political messaging and party posturing has seen an expert whitewashing of certain critical aspects of contemporary Indian history in the march toward a 'new India.' One such act by Modi, nearly unthinkable among reasonably minded people and circles, was to replace an image of Mahatma Gandhi, a near worshiped icon of national struggles for independence and freedom – with his own image – in a key symbolic venue [134]. Another action, seen as equally extreme, but subtle – vicious, and yet clever, is more prognostic still, of new directions for India. In a recent speech before the Indian Parliament, the Prime Minister did not mention one of modern India's well-known freedom fighters, and her first Post-Independence Prime Minister, Jawaharlal Nehru; [135] remarkable, considering that the speech concerned itself with a subject and action, which had intimately involved Nehru, whereby, both Mahatma Gandhi and Jawaharlal Nehru were imprisoned for their 'joined' action.

The reasons behind Modi's reluctance to speak of Nehru were two-fold. One, Modi had sure-fire intentions not to further elevate the account of histories and profile of personages associated with the Nehru-Gandhi political dynasty in the known space-time continuum [136]. Two, eventhough Nehru was well habituated with centuries old Hindu-Muslim rivalries in his time, he intentioned unity among the many population segments of what was to be post-independence India, and their peaceful co-existence in one India. Nehru promoted a philosophy of national unity through the adoption of the Ashokan principle of secularism.

Powerfully, and perhaps even insightfully, Nehru has knit himself into the very fabric of present-day identity of India; an identity too deep and weighty to either dislodge, or to deframe. A key example of the knit as described before concerns

Nehru’s involvement in the making of symbological choices for the national insignia, the Ashokan “Wheel of Law” [137] to be situated in the middle of the national tri-color flag, and “‘the lion’s roar of the Buddha’” as India’s national emblem [138]. Of the national flag with the Ashokan “Wheel of Law” as the centerpiece, Sadan Jha described its evolution as a *“triumph of history over the past, precision over ambivalence, singularity over multiplicity, standardization over fluidity and knowledge over the experiential dynamics of seeing”* [139]. Fundamentally, these value-centered perspectives and directions are at odds with the running perspectives of the day in Indian government and in many aspects of Indian public life.

Regardless of India’s rich evolutionary history, the bulky rise of intolerance, nationalism and isolationism, is now ever-present [140]. Alarmingly, Ram Madhav, the ruling political party’s (BJP) General Secretary, and Director of the India Foundation, proclaimed in a major national daily that, “[f]or the first time after independence, the dominant idea of India is rooted in India’s genius.” It is very difficult to parse the meaning of Madhav’s verbiage regarding “the dominant idea of India” in the first, and the idea of “India’s genius,” that Madhav is specifically referring to, in the second. That said, it is not difficult to comprehend what his next assertion means, when he stated that the liberals of India, have, as he put it, a *“palpable… demophobia — fear of the mob.”* Madhav went on to say that *“[t]he mob… are behind Modi. They are finally at ease with a government that looks and sounds familiar. They are enjoying it”* [141].

### 5.5 The *Aadhaar* program: a case of thriving political paternalism

The *Aadhaar*, India’s biometric ID program is said to be the largest such program in the world. At a 2014 conference in New York, Pramod Varma, Chief Architect and Technology Advisor to Unique Identification Authority of India (UIDAI), the creator and implementer of the *Aadhaar*, was heard saying that the inability to prove one’s identity is one of the biggest barriers that prevents the poor from accessing such things as the US$50 billion that India spends yearly on direct subsidies (food coupons for rice, cooking gas, etc.) to aid the poor [142]. At the very least, Varma’s ‘proof of identity’ apprehension is directionally mis-leading. By reading to this point, one will have arrived at an elemental deduction, which could potentially be associated with Varma’s own, that the UIDAI’s and indeed, the Indian government’s core anxieties relating to “authenticating” [143] a government benefit recipient is a valid concern. Reality is, there is corruption within the system of government disbursements; a severe country-wide problem, that the *Aadhaar* cannot, and will not technically fix. To this, Varma and others in the Indian bureaucracy have perhaps ignored the variety of reporting originating from India itself, on how problems such as pension fraud has persisted [144]. Corruption is the more dominant, entrenched and more persistent problem, somewhat of a custom, really, one that the Indian government cannot possibly wish-away by waving an *Aadhaar* wand, or by some illogical and wayward legislative act of churlish politicians who are generally moonlighting as “buzzword & bumper-sticker phraseology-fed” *Aadhaar* “sweet-sellers.”

Corruption within the system enables those intent on advantaging themselves to use that corrupted system’s mechanics and/or channels to one’s self-enrichment, through “fraud, waste and abuse.” Such things occur, even in more developed nation states and economies such as the United States, where “fraud, waste and abuse,” cost taxpayers a bundle, each year [145]. The *Aadhaar* cannot, and will not curb, or cure the systematized manner of corruption that has long existed in India; the cancer that is now eating India, from the inside out.

India is terribly ill equipped – technically, legally, and governmentally, to afford its citizens the protections that they need to actively participate in a globalized digital century. This author’s professional assessment is that the Indian Supreme Court took into account, diligently and perceptively, the country’s future economic predicament (its trade with the EU as an example), in terms of ICT, in their Privacy deliberations, before rendering a ruling related to Privacy’s status on the whole in India. Meanwhile, the Indian Parliament largely remains technically and operationally clueless, and doctrinally, organizationally, and electorally adrift regarding the implications of ‘being backwardly informed’ in this regard, leaving members of the Central Cabinet, with the ample opportunity to politically machine negative outcomes, such as the act of pushing the *Aadhaar* legislation through as a “money-bill*”* [146]. The European Union remains India’s largest trading partner, and the EU General Data Protection Regulation (GDPR) to be fully enforced by the Union in 2018, represented a high-watershed moment for India. Co-incidentally, before the momentous Supreme Court Privacy ruling, India did not have the prospect for placing forward, a countrywide unified system for data privacy and data security guardianship, active accounting, laying down modern laws and mechanizations for protections, auditing etc., etc., etc., that would meet or exceed international standards.

With respect to India’s future abilities to exchange information on European Citizens under the GDPR, if the Court of Justice of the European Union (CJEU) should rule against the employment of Standard Contract Clauses (SCCs) [147] that at present can still be relied upon to enable the transfer of sensitive personal information of EU citizens, such a ruling would be a big-blow for the Indian Tech Industry - hoping to rely on the ability to use SCCs as a work-around for the present day data protection conditions, systems and schematics that India presently has in place, in view of global standards.

While the message of 'creating self-sufficiency' [148] from Mahatma Gandhi's time is very pertinent and incredibly important to the national psyche even now, more fundamentally, fact remains that India's future economic prosperity is linked with globalized business environments that require India to be more interconnected with the rest of the world, and to be more modern. There is a vital need for those vestiges of old isolationism, and any of the entrenched "self-licking ice cream cone" style political machinery, economic assembles, and intemperate functionaries to be banished – to enliven the Indian Constitution and the accompanying legal, economic and social instruments, to the extent that data Privacy and Security needs can be satisfactorily met, and swiftly.

It must not be forgotten that unworldly and paternalistic politicians and other career government bureaucrats who have ostensibly sworn to uphold the Indian constitution, have been the ones insistent on the initiation and proliferation of a corrosively intrusive program, of which, they had possessed little to no understanding. Complimentarily, in argumentation before the Supreme Court, the Chief-Law Enforcement Officer of India, the Attorney General, cluelessly but, audaciously presented, that Citizens of the country had no absolute right to their bodies (See Figs. 16 and 17), and that upon demand by the government, a citizen had to submit to Government demands, in relation to the citizen's person.

Fundamentally, and with respect to Privacy and Security matters directly, the following realities surrounding the *Aadhaar* must be studied, if only to understand the need for consistent and constant vigilance on the part of populations against runaway instruments of governance.

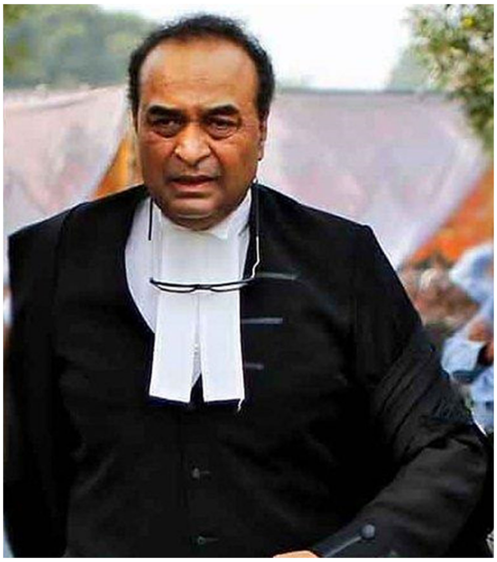
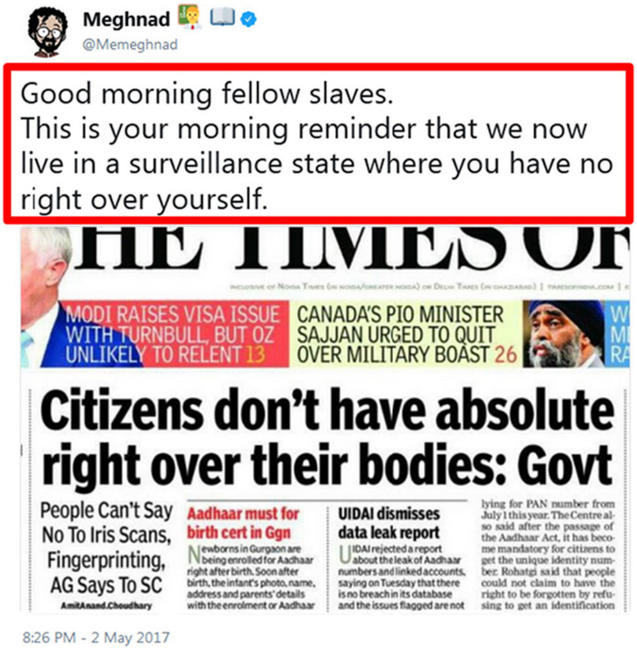


**Fig. 16** On July 22, 2015, Fmr. Attorney General of India, Mukul Rohatgi, Presented Before the Supreme Court of India That a Right to Privacy Was Not Guaranteed under the Indian Constitution. The Supreme Court Has Since Ruled Otherwise



Meghnad
@Memeghnad

Good morning fellow slaves.
This is your morning reminder that we now live in a surveillance state where you have no right over yourself.

HE TIMES OF

INCLUSIVE OF NOIDA TIMES (IN NOIDA/GREATER NOIDA) OR DELHI TIMES (IN GHAZIABAD) | TIMESOFINDIA.COM |

MODI RAISES VISA ISSUE WITH TURNBULL, BUT OZ UNLIKELY TO RELENT 13

CANADA'S PIO MINISTER SAJJAN URGED TO QUIT OVER MILITARY BOAST 26

Citizens don't have absolute right over their bodies: Govt

People Can't Say No To Iris Scans, Fingerprinting, AG Says To SC

AmitAnand.Choudhary

Aadhaar must for birth cert in Ggn

Newborns in Gurgaon are being enrolled for Aadhaar right after birth. Soon after birth, the infant's photo, name, address and parents' details with the enrolment or Aadhaar

UIDAI dismisses data leak report

UIDAI rejected a report about the leak of Aadhaar numbers and linked accounts, saying on Tuesday that there is no breach in its database and the issues flagged are not

lying for PAN number from July 1 this year. The Centre also said after the passage of the Aadhaar Act, it has become mandatory for citizens to get the unique identity number. Rohatgi said that people could not claim to have the right to be forgotten by refusing to get an identification

8:26 PM - 2 May 2017

**Fig. 17** Reaction from a Parliamentary Staffer after the Attorney General Pronounced Before the Supreme Court That Indian Citizens Had To Submit To Government Demands for Mandatory Iris and Fingerprint Scans on 2 May 2017

Some key facts related to the *Aadhaar* program launch are presented, and are as follows:

1) At the time of the *Aadhaar* program launch, the Republic of India did not have in place, a comprehensive, national Privacy and Information Security law that definitively asserted information privacy, safety and security protections commensurate to the type and scope of sensitive information that the Government of India wanted to acquire and use from citizens.
2) Prior to the *Aadhaar* program launch, Citizens were not informed of the potential risks related to Privacy, Safety and Security of highly sensitive Personally Identifiable Information (PII), its collection, distribution, storage, its authorized uses, or the possibility of compromises and risks of loss of PII.
3) Prior to the *Aadhaar* program launch, Indian citizens were not informed on types of recourse (if any) that were available to them, in the event of a PII compromise or loss
4) Indian citizens were prohibited from being able to bring complaints against the government in relation to the *Aadhaar* program's administration, operation, or maintenance.

How was it possible for the Indian government to bring into existence, a program that fails to protect the personal privileges of nearly 1.4 billion people in this way? How is the Indian government going to reign itself in, given that Privacy is a Constitutionally guaranteed privilege, and where government's unschooled and metagrobolized *Aadhaar* gaffers are still ebulliently 'sweet-selling' the phantasmical prospects of the *Aadhaar* initiative to the nearly 1.4 billion Indian citizens?

The *Aadhaar* legislation was bundled and introduced into the Parliament as a "spending bill/money bill," [149] which, without significant opposition, could stand a better chance of becoming a law. MP Tathagata Satpathy was the lone-voice of opposition to this money bill, and in-turn, the *Aadhaar* legislation within Parliament deliberations.

There are several other reasons as to why the Indian government was able to navigate the *Aadhaar* legislation concealed within a 'spending bill/money-bill' through the Indian parliament without much opposition. As MP Satpathy notes well in his Special Issue contribution [150], India is largely a *"Privacy unconscious State."* Satpathy also presses that his peers in Parliament had been supportive of the *Aadhaar* program deployment, in the majority.

There is another 'unsaid' reason as to why, such legislation was able to sail through the Parliament without so much as a whimper of opposition from the majority of the Indian lawmakers in both houses of Parliament, and for that matter, it is also largely the reason behind the absence of public outrage after the *Aadhaar* legislation was enacted. Going into that reason, the reader is reminded that Algernon Sidney had written in 1698, to remind, *"[g]overnment is not instituted for the good of the governor, but, of the governed; and power is not an advantage, but a burden"* [151]. To understand the character of that power, we must understand, how in India's case, it is constituted, and why it is used in the manner, it is.

UNESCO has determined that 37% percent of the world's illiterate live in one region of the world; they live in one single country – India [152]. UNESCO's report also detailed that in India, less than half of children are learning the basics, placing India in a category where the learning crisis is now extensive [153]. This profoundly limits even the minimal participation of Indians in a Digital Century, not to mention that the same in society will also be unaware of the many components that make-up the digital ecosystem in which they too have, or will have, a significant foot-print. At a minimum, this debilitating statistic can only be seen as 'a paralytic agent,' being administered slowly to a segment of Indian society, where many have consequently been rendered incapable of evaluating properly, 1) the individual Privacy and Security risks in the Digital Century, and 2) the array of long-term impacts from their participation in the government mandated *Aadhaar* program, among other things. In keeping with Sidney's statement – Power can only be focused and used for the good/benefit of the people, when populations are educated, made knowledgeable, and are empowered to act upon the knowledge they possess for a larger national good.

How has the Indian government served the Indian people, in accordance with the Indian constitution, in the case of the *Aadhaar*? A larger and perhaps more persistent question is, how does the Indian government hope to emerge the subcontinent as anything more than a regional economic power? How will the Indian people get beyond massively tribal mentalities, crippling illiteracy, lack of fundamental respect for human rights, social disorder, and incivility?

### 5.6 Privacy and security in the time of mob lynchings, vigilantism, and witch hunts

Within a country whose Constitution presently states that it is a "Sovereign Socialist Secular Democratic Republic," 'Secularism' seems to be on the outs, as vigilantism and lawlessness has become quite a common place in modern India. "Cow Vigilantes" – in 'Hindu-on-Muslim' violence have imposed staggering consequences that outwardly expresses a colossal contempt and disregard for rule of law. One Indian newspaper noted recently that since 2010, 86% of all those killed in cow-related violence (See Fig. 18) have been Muslim, and 97% of all attacks have happened since Narendra Modi has been in power and 52% of the attacks were based on rumors [154].

In 63 cases, 28 Indians have been killed, and over a 120 injured. In the first six months of 2017 alone, there were 20 "cow-terror attacks;" more than 75% of the total 2016 figure [155], and there seems to be no end in sight. The author wishes to note, perhaps mischievously that a reporter claimed by way of a reputed worldwide broadcaster that, *"the lynchings are giving Narendra Modi's government a bad name"* [156]. The author would cheekily submit that "a bad name" for Modi should be an item of least concern for all Indians. Perhaps it is not apparent to those in the Indian government, civil leaders, and others, in, or about the thrones of power that the savagery emanating from many corners of India has diminished India itself. There is no going back. The criminal, cowardly, reprehensible, and debauched acts that are being carried out in the name of religion, in a State that claims itself to be "secular," will only go forward to confirm Winston Churchill's wholly

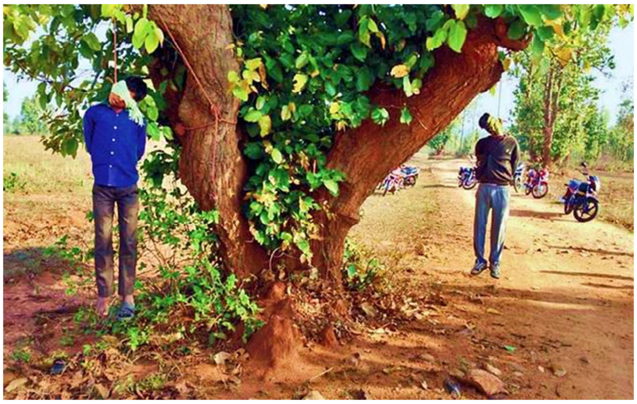


**Fig. 18** [*] Lynching of Innocents in India by Cow Vigilantes. Photo: Somnath Sen

offensive statement regarding Indians, from a long-gone era, where he spouted, *"… [t]hey are a beastly people with a beastly religion"* [157].

Many of the savage and beastly acts of murder and mayhem have also been televised in "Bollywood" style media segments to many parts of the world, by Indian media outlets themselves [158]. Foreign broadcasters (outside India) have re-broadcast segments of that reporting from Indian broadcasters also [159]. Series of political killings [160], silencing voices of reason in opposition [161], execution of outspoken journalists [162] have all become very prominent activities. How is it possible to be a Republic, where "the law" can be seen to be an integral part of the tapestry of mayhem and destruction? How are the very best intentions imbued into a constitution to be upheld by weak governmental structures and leadership, weak command and control structures, not-professionalized/poorly trained/unethical law-enforcement officials who are many times party to offenses and crimes that include rape, murder, rampant scales of corruption, and are party to events that demonstrate no respect for human life?

This is the environment in which, India has to consider now, how to proceed toward implementing 'Personal Privacy' protections. India has initiated a "Giant Leap for Mankind" regarding Privacy. However, as a nation, perhaps it is the least prepared to offer its citizens the very protections they must absolutely be afforded. The educated masses of India must now act, and lift an entire country out of quagmires ignorance has made to exist, those that cloud the country's promising futures. India's bureaucrats will be well advised to remember Mahatma's gift of a social conscience to the future of India; one that is incorruptible. His talisman for successive generations constituted a simple instruction, to be deeply introspective, regarding forward actions. Mahatma said,

> "Whenever you are in doubt, or when the self becomes too much with you, apply the following test. Recall the face of the poorest and the weakest man whom you may have seen, and ask yourself, if the step you contemplate is going to be of any use to him. Will he gain anything by it? Will it restore him to a control over his own life and destiny? In other words, will it lead to swaraj [freedom] for the hungry and spiritually starving millions?" [163]

In terms of the UDHR more basically, and all relevant concerns associated with the proper establishment of internationally relevant data Privacy and Security measures oriented to empower Indian citizens to 'self-sufficiently' participate in the digital economy and the digital century, Mahatma's foundational and encouraging counsel should be heeded. All in all, regardless of India's rich history that once pointed to ways of good government, and the most current national claim to be a secular government - among other things, and the recent ruling by the nation's Supreme Court, India is still ill organized to provide its citizens the privacy and security they will need, both from a human rights perspective, and as a constitutionally mandated right.

## 6 Surveillance, interdependence and interconnections

> "Experience should teach us to be most on our guard to protect liberty when the Government's purposes are benificent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding." – Louis D. Brandeis, Associate Justice - United States Supreme Court *(Olmstead v. United States)*[45]

**57** years after Justice Brandeis wrote the aforementioned statement, U.S. Supreme Court Associate Justice William J. Brennan Jr., stood before the graduating class at Brandeis University in Massachusetts, to deliver an unambiguously stern warning that the *"modern age posed special dangers of Government encroachments on freedom"* [164]. In a time much before the data-rich forces[46] of Facebook, LinkedIn, Twitter, Instagram, Pinterest, Tumblr, Reddit, Skype, WhatsApp, Snapchat, Tinder, Wickr, YouTube, etc., the 80 year old Jurist delivered a final instruction to the departing class that the threat to the free-society that is the United States lay in that 'suchness,' where *"we have given Governments more power over our lives than ever before"* [165] … and to the quiddity in that suchness, where "*we seem not more concerned, but more indifferent to the consequences of this surrender"* [166]. In his address, Justice Brennan re-iterated Justice Brandeis's decipherment of society's prime 'personal freedoms' challenge, pronouncing with an unwavering tenor that *"'[w]e seem to have forgotten Justice Brandeis's admonition, '[e]xperience should teach us to be most on our guard to protect liberty when the Government's purposes are benificent.' '"* [167]

Yet another generation since Justice Brennan's re-registration of Brandeis's initial written act of dissuasion in *Olmstead v. United States,* 'the conviction' embedded in Brandeis's dissent should appeal to us all the more, be more relevant, and found to have been made brilliantly and beautifully timely. Yet, that which we observe constantly and consistently is that there are insidious invasions of liberties all around us, and we are culpable in the surrender of our personal freedoms. We gladly cede

[45] *Olmstead v. United States,* 277 U.S. 438, Decided 4 June 1928 https://supreme.justia.com/cases/federal/us/277/438/case.html

[46] The matter of intrusiveness will be discussed briefly, within section 6

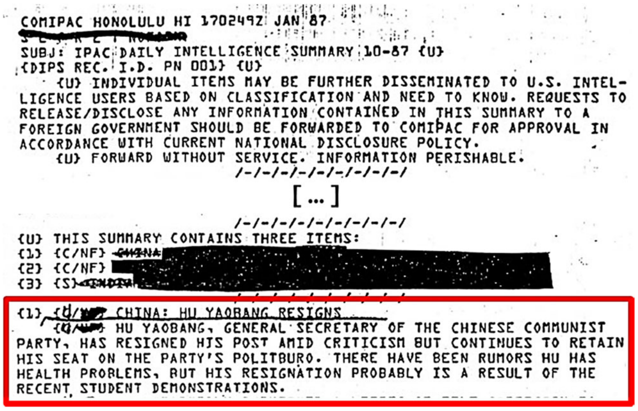
freedoms to others in exchange for a smidgen or two, of trifling gewgaws, and an even more egregious act, viler and more contemptible, is that act which Justice Brennan had been uproarious of, when he said, "*we seem not more concerned, but more indifferent to the consequences of this surrender"* [168].

Nowadays, we are the 'least-on-our-guard' against the elements to which Justice Brandeis's premonitory avowal, and Justice Brennan's **57**-year exhortational follow-up to that which Brandeis had once pointed. And, despite humanity's encounters with 'slips-and-slides,' people have the inherent capacity to overcome[47] the worst atrocities levelled against them. Modern-day Rwanda is an outward example of such a 'turn-around.' On the other hand, despite our inherent capacity to overcome, borrowing from Brandeis, the tensions between *"men born to freedom … [who are] alert to repel invasion of their liberty"* are bound to suffer an unending tensions and conflict with *"evil-minded rulers."* In such regard, the world once witnessed a type of a "power of the people" expression in China, during "the June 4 incident," at Tiananmen (See Fig. 19). A number of events, more than those that met the public eye, seeded the occurrence of those events of 4 June 1989, which originated in 1987 (See Fig. 20), and changed the very 'texture of Politics' [169] in China. The death and funeral of reformer, and Party General Secretary Hu Yaobang's in 1989, triggered an outpouring of affection from student demonstrators who were in support of reforms Yaobang had wanted see initiated - that June, spawning the Tiananmen confrontation. Many in Chinese Committee ranks considered the Student protests to have been unsuccessful then. In times that are more recent however, the 19th National People's Congress has once again turned China toward a "strong-man" hardline archetype for the years to come. Moreover, the inertia within those bodies of College/University Students that were once behind social and governmental reforms have been dissipating due to government crackdowns ordered by new Chinese leaders since Tiananmen [170], combined with people's fading historical memories, diminishing degrees of political consciousness and actions by people [171]. That is how freedom always dies, drawing its nourishment for growth from apathy.

Today, with the National Development and Reform Commission, and People's Bank of China leading the planning of the system, the government of China, with 35 of its government departments cooperating and supporting it, the "Construction of a Social Credit System (2014–2020)," [172] is fast underway, covering four major fields of public life: politics/administrative affairs, business/commercial activities, society/social behaviors, and the justice/judicial system. The rationale provided by the government for the deployment of this system to fit 1.3 billion people of planet Earth is, that, China's national security is at stake, and that China's population is suffering from a moral and ethical compromise and decline. The conversational perspective that the Chinese government has put forward to advance the instantiation of the system is simply that *"[w]hen people's behavior isn't bound by their morality, a system must be used to restrict their actions."* In the assessment of this author, with this system, the government will aim to monitor, and evaluate - all present and future Communist Party members, ensure Party cohesion, cement party loyalty, conformity, and social order in general,. It is intended to be a Party instrument, a foundational system for political control. Whether citizens of China will again assert their inherent powers remains to be seen.

**Fig. 19** Photo of The "Tank Man" (Wall Mural), Tiananmen Square. Mural Photo taken - 5 June 1989. Source: Public Domain

The author is compelled to consider a bit of Jeffersonian wisdom therefore. In a personal correspondence, Thomas



```
COMIPAC HONOLULU HI 170249Z JAN 87
[redacted]
SUBJ: IPAC DAILY INTELLIGENCE SUMMARY 10-87 {U}
{DIPS REC. I.D. PN 001} {U}
    {U} INDIVIDUAL ITEMS MAY BE FURTHER DISSEMINATED TO U.S. INTEL-
LIGENCE USERS BASED ON CLASSIFICATION AND NEED TO KNOW. REQUESTS TO
RELEASE/DISCLOSE ANY INFORMATION CONTAINED IN THIS SUMMARY TO A
FOREIGN GOVERNMENT SHOULD BE FORWARDED TO COMIPAC FOR APPROVAL IN
ACCORDANCE WITH CURRENT NATIONAL DISCLOSURE POLICY.
    {U} FORWARD WITHOUT SERVICE. INFORMATION PERISHABLE.
                           /-/-/-/-/-/-/-/-/-/
                                  [...]
                           /-/-/-/-/-/-/-/-/-/
{U} THIS SUMMARY CONTAINS THREE ITEMS:
{1} {C/NF} [redacted]
{2} {C/NF}
{3} {S}
{1} {U/[redacted]} CHINA: HU YAOBANG RESIGNS
    {U/[redacted]} HU YAOBANG, GENERAL SECRETARY OF THE CHINESE COMMUNIST
PARTY, HAS RESIGNED HIS POST AMID CRITICISM BUT CONTINUES TO RETAIN
HIS SEAT ON THE PARTY'S POLITBURO. THERE HAVE BEEN RUMORS HU HAS
HEALTH PROBLEMS, BUT HIS RESIGNATION PROBABLY IS A RESULT OF THE
RECENT STUDENT DEMONSTRATIONS.
```

**Fig. 20** Excerpt of Declassified Cable from Command Intelligence Center Pacific (COMIPAC-Honolulu, HI) on Party Gen. Sec. Hu Yaobang's Resignation. Source: National Security Archive

[47] Not to be confused with imprudently or obtusely setting-aside, glossing-over or culturally whitewashing acts of atrocities or inhumanity, or otherwise succumbing to flavors of revised and more comfortable forms of histories

Jefferson once provided some founding-fatherly advice, saying, *"I know no safe depository of the ultimate powers of society but the people themselves, and if we think them not enlightened enough to exercise their control, with wholesome discretion, the remedy is not to take it from them but to inform their discretion by education"* [173]. In Jeffersonian spirit therefore, the author will aim to demonstrate for the reader and attempt to enlighten upon the unusual web of interconnections and interdependence between key players on the Digital stage, the nature and texture of surveillance potential and/or political control; the susceptibility of modern populations to agents, mechanisms, methods, depth, scope and the opportunities and the frequency of surveillance. The only vaccine for the susceptibility (in whatever manner) and as mentioned is, the peoples' acquisition of knowledge, which in turn shall permit their 'exercise of control,' to which they are rightfully entitled, aided by their wholesome discretion - acquired through a proper education.

### 6.1 Road to 'high trials' in privacy and security

That which seemed unthinkable before, has yet again happened. Building and assembling information infrastructures such as undersea fiber-optic data cables have long been the province of joint ventures, and large consortia of telephone/telecom firms. Such associations were necessary because beyond the costs of just placing an asset such as an undersea cable into service, there are many other costs related to business activities as client and capacity administration, management and maintenance, and various business risks that require distributed adequately to realize profitability from operations. So, what type of a message is telegraphed when an unconventional trio organizes to build something that, just **2–3** years ago would have been thought as an eccentric and cracked business decision? What would be the answer? For one, the expected business return must have been seen as an activity worthwhile doing, and the other reason probably had to contribute in some way to operational stability and reliability.

The trio of Facebook, Microsoft, and Telxius (a Telefónica subsidiary), have just completed the installation of the highest-capacity data transmission cable to have ever crossed the Atlantic. The cable, 'MAREA,' will connect Virginia Beach, Virginia (U.S) and Bilbao, Spain (another first), at a speed of ~160 Tbps.[48] Facebook and Microsoft anticipate a healthy jump in their data capacity needs, which would have been difficult to acquire in the commercial market at present. Total U.S. undersea international cable capacities topped ~120,000 Gbps.,[49] [174] and ~87% of that total capacity is already active [175]. It quickly becomes obvious, as to why, Facebook and Microsoft and Telxius joined-up in this venture. We know that from data that Google has gathered from Android users around the world and released, that 93 million selfies are taken each day, and devices that have Android installed as an OS are checked 100 billion times a day! [176] All those selfies, e.mails, Facebook posts, Instagram picture of lunch, WhatsApp calls/messages, Skype connections etc., need to be transported to interesting places. One can imagine of the rising Privacy demands that correspond to the climbing data rates and capacities. To be sure, to assure the safety and security of information throughout its use cycle, at either ends of such cables are institutions, organizations, people, processes and technology, all organized to interoperate competently, and is a running concern globally.

The world expects workforces to have wholesome, high quality learning and practical knowledge, which would consequently advantage those others, who are likely to receive services from them. Accordingly, in the Digital Century, the inviolability of Privacy and Security of information is principally fastened to an individual's 'internalized knowledge' of information systems, informational backgrounds and practical information handling situations, appreciation of attentiveness to detail, action and reaction potentials, evaluating sense for cause and effect, self-control and self-restraint, among other qualities. Expressed in a different way, in the coming days, it would need to be made evident for one and all that those in society to whom we entrust our personal and private information will be able to regard, handle and safeguard information, in all the ways that would be needed, to ensure the safety and security of personal and private information for which others accept custodial responsibility, in addition to their professional specialties.

However, what if the evidence of being able to maintain the safety and security of conveyed information, or the continued assurance of its safety is not available, nor will it be possible to obtain? How should anyone act, or react? The scope of this writing is unfortunately restricted to revealing only a sub-set of the comprehensive risks, which, when and if given the opportunity to take hold and ripen, can still make Personal Privacy and Security of information incredibly vulnerable. An immediate fulfillment of the most basic understanding concerning how risks compose, and how the composed risks then have the potential to affect operations of critical Privacy and Security preserving components, institutional segments, or divisions and their respective informational ecosystem must exist. There is also the necessity to be acceptably configured to be able to address rapidly proliferating risks within the informational ecosystem through threat/risk management and mitigation strategies.

[48] Tbps – Terabits Per Second 1,099,511,627,776 bits per second

[49] Gbps – Gigabits Per Second 1,073,741,824 bits per second

In the interest of suitably considering Privacy and Security risk mitigation and management strategies, we must patiently consider many underlying organizational and operational information. Some of those organizational and operational considerations are viewed within this Editorial Chapter from a human resource centered perspective. Human Resource executives and managers straddled with the responsibility of furnishing enterprises with properly qualified and competent staff are acutely aware of the many workforce related problems. Some of those problems will be situationally addressed here, in view of rising Privacy and Security demands. As is, aspects addressed in this section represent very real problem-spaces for society's forward march into time, with technology as co-traveler, and with populations that are not versed to realizing and comprehending, the philosophical, social, moral, economic, technical, safety and security parts of technology, and technology related-use, which when configured correctly, can originate benefit to society, as in terms of data privacy and security.

### 6.2 Selected sociographic representation of the millennial workforce majority in terms of privacy and security futures

To protect Personal Privacy and Personal Security properly, a wholistic examination of problem dimensions within modern surveillance societies must be made, especially the many qualitative features of those who are targets of surveillance must be made known. To begin, let us reflect upon the common reality that the demographical composition (diversity and education), the temperament (personal capacities and capabilities), integrity (commitment and quality output) of the global workforce is changing. In the United States, Millennials (18–34 yrs. of age in 2015) had surpassed "Baby Boomers" (51–69 yrs. of age in 2015), as the nation's largest living generation – 75.4 million, as opposed to the 74.9 million Baby Boomers in the USA [177]. Fundamentally, in the United States at least, this epochal shift has vividly altered the outward complexion, and the innermost constitution of the workforce. In the context of this epochal shift, and all else that form associated considerations (economic, as an example), including the Privacy and Security angle as well, the following aspects will be highly relevant for the United States – as it will be, for the rest of the world. Here and now, how those who are doctors, nurses, teachers, judges, lawyers, carpenters, policemen, computer programmers, plumbers, contractors and spaceship builders, deliver qualitative and quantitative services (in this case, assuring the personal safety, and the security of personal privacy information), is for all of us to grasp, to appreciate, or to remediate as a society, if and when necessary.

*The Millennial Generation/'Digital Natives'*, and *'Generation Z'* [178] too, perceive those that are part of the 'Greatest Generation,' the 'Baby Boomer Generation,' and even 'Gen-Xers' as "digital immigrants*"* [179]. The underlying impression commonly "offered-up" is that, *'Digital Natives'* are appropriately placed in space, time, and just so - in the chain of human evolution where, somehow, their generational configuration[50] aid and bolster them uniquely to indispensably enable societal digital transformations everywhere. The author completely rejects any arbitrary notion that idly proposes that 'Digital Natives' are either wholly proficient, knowledgeable (especially), or both, where their technology use is concerned. The author does concede that there are likely exceptions, as in other cases. More often than not however, that which is presented commonly is an artificial conflation of riotously differing authenticities *(comfortability v. proficiency),* by no-doubt, well-meaning parties.

Conflations aside, as concerns Digital Natives, it is plausible that they are more 'at ease,' in their use of technology.[51] There is a difference between being comfortable with the use of technology and being proficient with the use of technology. Of course, a person can be both comfortable, and proficient, in the use of technology. The chasm between *comfortability v. proficiency* (and there is a chasm) in relation to technology use must not be casually dismissed as though there is not one, for there surely is that. Consider as an example - it is possible to be fluent in a language (mostly in a colloquial sense), and still use the language, gracelessly and downright offensively. Technology use *comfortability* is no substitute for *proficiency*, at work. In view of these and other points, a brief discussion of the widely visible lack of preparedness in today's workforce can serve to be a cautionary note to Privacy and Security planners, and practitioners. Furthermore, the discussion can potentially sensitize parties to, the nature of the demand for qualified and capable staff configurations to suit institutional preparedness, and by that, effectiveness in data safety and protections.

Enterprises that have significant dealings with Intellectual Property, various forms of proprietary information, highly sensitive personal/institutional information, and or classified information, have very legitimate reasons to at least be apprehensive of misguidedly hiring a thief, to be the "ship's" (enterprise's) purser. Whether preservation of Personal Privacy, the Security of sensitive information, or some other purpose is the central mission, modern organizations strive to design a *gestalt* – in human resources that shall succeed in the delivery of mission centeredness, and mission successes. In contrast, advancing confutations for hiring a thief, as the ship's purser

[50] "The configuration" refers to the purported ease with which they (Millennials and Generation Z) use tech, or that "comfort they exhibit" in relation to interfacing with technology, and use

[51] This particular point will be discussed later in the section, "8.3. Righting The Perspectives on Modern Workforces"

will likely be most unwelcome, especially while an enterprise is on its way to insolvency.

In relation to Digital Natives then, the author has chosen to present an aspect of the awareness and understanding that the U.S. legal community has gained on Millennials, given that community's sensitivities to key items to be considered in relation to the standing-up of 'Juries' for court trials. In *"The Generation X and Y Factors,"* [180] authors who are Courtroom-trial strategists have written to advise trial litigators interpreting Juror selection considerations, and of tangible actions to be taken before impanelling Juries, especially when Generation Y candidates may have to be impaneled. In the article, the authors characterize Generation Y (Millennials) as the "entitled generation," "naïve," "whiny Peter Pans, nurtured by helicopter parents," "demanding," "poor communicators," "socially digitally connected," "distractible" ("prone to suffering "withdrawal symptoms from not being "connected" while on a jury."), [having] "short attention spans," and as "the products of the "everyone gets a trophy" mentality." The authors also note importantly that, "Generation Y rarely challenges the reliability and source of information," and finally, that "[their] entitlement character, juxtaposed with their underemployed and unemployed status, [would create] … a Jekyll and Hyde dynamic." Through their writing, the authors have attempted to alert and instruct their peers to the need to compensate for these potential Juror characteristics.

#### 6.2.1 Digital behavior characteristics of millennials in relation to privacy and security futures

Societal use of Information and Communications Technology (ICT) to realize productivity, to achieve quality in professional work, and in personal life, has dramatically increased in the span of a single decade. The arrival of smartphones, development and growth of applications, fast growing radio spectrum use - spawning greater voice and data application development, and convergence of technologies have all made that which was once impossible, now possible. Notions of "possibilities," have fueled individual, collective, and global "informational thirsts," and the many ways by which we consume our "bits of data" daily. On one hand, these "thirsts" have rudimentarily altered, re-formed, and improved humankind. On the other hand, the same "thirsts" have transfigured, misshaped, tainted, and fouled our professional and personal ecologies. Those foulings are now threatening the very fiber of Privacy and Security operations in enterprises, and at a practical level, the same are functionally affecting various age groups in our society, especially millennials. Some of the contributing elements to the aforementioned problem areas will be examined below.

#### 6.2.2 Informational access behaviors and their relationship to the future of privacy and security

The Mobile Mindset Study [181] broadcast that 'a new mobile mindset' had materialized in societies, largely shaped by many technologies and types of technological use, where our emotions, thoughts, and behaviors are for instance, predisposed to being molded by the presence (or at times by the absence) of smartphones. The survey uncovered that 80% of all men felt either *'desperate'* or *'panicked,'* as compared to 94% of women, who acknowledged feeling that way upon their discovery that they had misplaced their smartphone. Such is the nature of behavioral response, when we misplace an 'extension of our physical selves;' yes, an extension of our physical selves [182]. 54% of those surveyed admitted to being on their phones checking it while lying in bed: before they go to sleep, after they wake up, and even in the middle of the night. 40% of those surveyed admitted to checking their phone while on the toilet; 30% admitted that they checked their smartphones when having meals with others; 24% used their smartphones while driving, and nearly 10% of those surveyed used their phone while in a house of worship. This is the type of unacceptably aberrant mindfulness and etiquette that users have developed through their seemingly "routine engagement" with mobile technology. If that were not enough, the study noted that many people have reported as having experienced *"phantom smartphone twitches: the perception that [the] phone is ringing, buzzing or bleeping even when it's nowhere in sight"* [183].

#### 6.2.3 Frequency of access to digital devices, interruptions, and productivity lossess at work

The frequency and range of technology use[52] has completely immersed us into an 'alternate universe,' and has managed to create perversions in societal norms. Take into consideration an observation Tomi Ahonen, formerly of Nokia made. Ahonen said that people check their phones ~ **150** times in a day, which translates to **~6.5** times every hour [184]. All should wonder, how real "work" is going to be done, when there are so many interruptions in the span of one hour, and where there is a likely call for 'a response' with each interruption, and in either direction. If a worker has to attend to a demand from his/her employer for a solution that corresponds to a daunting problem, how could the worker provide to that problem - the proper mulling required, notably when the employer demand has to compete with those smartphone interruptions. In the

[52] The high frequency and range of technology use (immersion) has seeded and industrialized, a range of conditioned responses in users, as in the case of phantom mobile phone twitches, buzzing and ringing etc.

United States, there are employers that mandate employees to not have a personal telephone on their person at any time during work hours, or at any other time while on company business. Many employers in the United States also mandate employees to not take, or make personal telephone calls while at work. However, there is no one universal approach taken by employers to curb unproductivity, interruptions, and disruption in the workplace from personal telephone use.

Science tells us that even an interruption less than 3 s (2.8 s) in duration will "double" the sequential error rate on a certain task [185]. Longer distractions such as a 5 min phone call is likely to take more than 20 min beyond the distraction itself, for one to be able to return to that point before the distraction [186]. Accordingly, with the high compulsion to be connected, and/or to check one's smartphone as much as ~6.5 times an hour, how is any work done? Distractions and Errors can be prime causes for Privacy breaches. Various studies including one from the Computing Technology Industry Association (CompTIA) routinely found (especially since 2004), that "human error" is primarily responsible for industry security breaches/privacy breaches and that "management of human error should be of high priority in organizations*"* [187].

Beyond distractions and interruptions themselves, is the subject of access to social media and other digital services for personal use, by one's own volition. Information that particularizes workplace productivity losses in relation to social media use at work is available, but not so much in depth. An example of that which is available in from 'Harris,' that interviewed 2000 hiring and human resource managers, and more than 3000 workers (18 yrs. +) in the U.S., on behalf of 'CareerBuilder,' uncovering that social media, cell phone/texting, Internet use, have all been identified as productivity zappers in a not well managed firm. [188] A Worldwide Kelly Services appraisal of 168,000 people from 30 countries [189] show that 49% of all surveyed specifically indicate that Social Media use at work, negatively impacts work output. Members of the Baby-Boomer Generation, Generations X & Y have all expressed decisively that Social Media use at work negatively affects productivity. Just the same, some ***30%** of all interviewed had indicated that they feel it is appropriate to access social media for personal use - at work.* Again, this is the nature and texture of work ethic and personal commitment in emerging workforces. Such reflections must be at the core of workforce related planning, both in national security circles, and as they must be - outside of governments - in places like doctor's offices, hospitals, genetics labs or schools, where the likelihood of extremely sensitive personal information being available, and the risk of exposures are both very high.

#### 6.2.4 Psychosocial characterizations of the digital workforces in relation to informational access and use

It has been made clear that social media uses are more 'addictive' than cigarettes and alcohol [190]. Followingly, the world's "unnatural" and "addictive" attachments to digital adjuncts have augmented boundaries in sociology and psychology, where new nomenclatures have now surfaced. Terms like *NOMOPHOBIA* [191], *PIU (Problematic Internet Use)* [192], *IGD (Internet Gaming Disorder)* [193], *Internet Addiction Disorder (IAD)* [194] and *FOMO (Fear Of Missing Out)* [195] etc., now populate and color the Digital Century' lexis. The additive capability of the many tools in the Digital Century tool chest is of high concern to this author, specifically in terms of how addictions and distractions will increase the frequency and the scope of Privacy and Security compromises, not to mention the required productivity from employees at work. With expressed concern of addictions, a child health, behavior and development specialist at the Seattle Children's Research Institute noted that, *"[g]iven our current understanding that there is a genetic predisposition to behavioral addictions, we may be going a long way toward ensuring that the entire susceptible population develops them [digital device & services related addictions]"* [196]. An individual's susceptibility[53] is an important consideration that the author will be addressing, as a way of demonstrating the need-be areas of sizable concern in the pursuit of protecting Personal Privacy and Security. Susceptibility[54] is a crucial psychological and sociological area of concern insofar as digitally connected individuals are concerned, especially if they are to be entrusted at all with sensitive information of any kind, which require prescribed handling, and protection.

Formally, there are few venues where a worker's "digital addictions" has the prospect of being addressed effectively. No matter whom the employer, whether they are schools, hospitals, courts, the military, religions entities, and/or corresponding houses of worship, people have to be - both broadly and deeply concerned of such addictions. In many parts of the West, Internet Gaming Disorder, or Internet Addiction Disorder etc., are not recognized as mental health problems, whereas Italy, Germany, France, Korea, Japan, China, etc., are attempting to address it keenly as nationally relevant mental health concerns. As mentioned just before, since there are no

[53] The author is referring to 'susceptibility' here in a way to explicitly state that someone could be 'compromised' psychosocially, to be manipulated, deceived, or be otherwise impressioned by their engagements and activities with others over digital devices. It also infers to that tendency in one to become mischievous, corrupt, or to be malicious due to such compromise. The author also intends 'susceptibility' to signify one's inability to apply critical discretion in specific situations, or that inability to resist another's action(s) to surveil

[54] *Ibid*

formal treatment pathways that are sure to yield in the most effective outcomes for such issues, just a few treatment centers in the U.S., have been internally considering the matter, just enough to have at least a small footprint in the area [197], whereas, China is home to the Internet Addict's Bootcamp [198]. Such are the type of concerns that must find its way into all meta-Privacy and meta-Security considerations and configurations this day. The author has already written of actively employed healthcare workers in the United States, who routinely did not perform their work as assigned in a healthcare facility, having wastefully spent their work times on digital devices [199]. Can we expect persons who are under the control of personal compulsions, and/or the prevailing nature and types of digital addictions, to be ethically and morally responsible for anyone's private information, if such people were entrusted with it? Would it be plausible for susceptible persons in the workplace to mis-use/abuse protected information that is entrusted into their care?

In our societies, the existence of laws, frameworks and instruments of enforcement for those laws, and the presence of societal/professional norms and mores have generally posed a preventative effect (as an example), on alcohol and drug use at work [200]. As a way to understand that the ground upon that we have stood all this while has changed, it is important to note how dramatically, the aforementioned ecosystem has been altered. We should note that 70% of the ~15 million Americans who use illegal drugs are employed. This means, those Americans bring their habit to work. To crystalize that point, we should review that a large U.S. federal survey has demonstrated that nearly a quarter of all U.S. workers reported drinking during the workday at least once in the past year [201]. According to the National Council on Alcohol and Drug Dependence (NCADD), the problems that c/would accompany an employee with addictive behavior and habits into the workplace, are the following. They are: tardiness/sleeping on the job, after-effects of substance use (hangover, withdrawal) affecting job performance, poor decision making, loss of efficiency, theft, lower morale of co-workers, increased likelihood of having trouble with co-workers/supervisors or tasks, preoccupation with obtaining and using substances while at work, interfering with attention and concentration, illegal activities at work including selling illicit drugs to other employees, higher turnover etc [202].

In the case of constant texting/sexting or social media access at work, although organizations are attempting to adapt, still, few U.S. organizations have 'top-to-bottom' - tangible and unambiguous policies, and/or management action frameworks regarding the use and abuse of employee owned devices (tablets, cell phones and laptops brought into the enterprise under a BYOD[55] plan), or company provided mobile devices [203]. Although there are management and auditing "schemes" in many organizations, to prevent the risk of exposure, loss of privacy and security of data more generally, in light of the *"degree of depravity in mankind which requires a certain degree of circumspection and distrust"* [204] it is worthy saying that protective schemes have a long way to go still, given the seemingly limitless landscape of data collections, data keeping, manipulations, and use.

### 6.2.5 Digital predispositions effecting privacy and security cause for concern and guardedness: insiders who are unaware they are a threat

While people outwardly express great concern and contempt for violations in privacy, the same parties often avail themselves to data services with little concern for privacy, and are also many times, completely unconcerned of privacy all together [205]. Taking a wide-angled perspective of Privacy and Security, given that, today - those in government and industry are required to protect the personal data of others that they handle, institutional pathways for protections must exist that will be able to endure assaults, and attempts at infrastructure infiltration, and data exfiltration. The very same protective methods and means must also 'combat' the proclivities of those persons that work in government and industry[56] to compromise the safety and security of others' Privacy. Will organizations succeed in their efforts to combat deep-rooted and undesirable 'psychosocial' personal tendencies? This is a vastly different question than the one that people and organizations are generally disposed to asking currently, when references to "insider threats" are made. The dimension surfaced below is one often omitted, or unperceived, winked-at, pushed-aside, varnished or simply camouflaged due to the nature of an organization's misunderstanding of standing issues, overall unpreparedness to meet threats, or most importantly – the lack of internal experience and expertise.

Let us examine a few more underlying and contributing psychosocial vectors, which complicate those measures undertaken by organizations to curb informational exposure, and any loss of Privacy. It was stated before that the subject of susceptibility would be explored more. While the many aspects of personal susceptibilities cannot be fully explored here, or be restrained only to that context as it could be applied to the safeguarding of Privacy and the Security of information that belongs to others, the following dimensions will be helpful to surface. Consider that Studies have revealed that there is a linkage between "Internet usage," "dissociation" (time distortion), "disinhibition," and "psychoactivity" – which in turn promotes and

[55] "Bring Your Own Device"

[56] Insider threat

cements highly addictive predispositions. Thus, it is important to ruminate upon the following findings.

In *"Psychological characteristics of compulsive Internet use: A preliminary analysis,"* [206] responses from more than **17,000** people were analyzed, revealing that **83%** of those whose answered met the criteria for Internet addiction, having reported "loss of boundaries," while **39%** of 'non-addicts' also reported the same condition. Moreover, in the study, **80%** of the respondents who were addicted - reported "disinhibition," as opposed to **43%** in the case of 'non-addicts.' In the case of "dissociation" (time distortion), the probe disclosed the non-addicted in the group, admitting to *"sometimes loosing track of time,"* while the addicts described that they lost track of time, *"almost always."* At this juncture, the reader is re-directed to those comments made earlier, which relates to employee loss of productivity at work, where employees find themselves distracted, or otherwise pre-occupied by non-work related Internet activity. The frequency with which people access social media outlets, and the tendency for workers to 'barefacedly'[57] interface Internetted resources at work, which are non-work related, causing productivity and employer/job outcomes to suffer as a result is perhaps well explained by Ellen Toronto [207]. Toronto, citing Ogden,[58] says this dissociation from the real world and attachment to the fantasy world is a representation of *"an impairment in symbolic thinking, a concretization of fantasy,"* where *"a dissociation of fantasy and reality, a state in which one [state] no longer informs the other,"* and where *"[t]he mind loses its capacity to move freely among affective and intellectual elements".* Moreover, Toronto says, the dissociation then *"draw[s] us away from the essential characteristics of human development"* John Suler [208] has proposed that such detachment, such dissociation from the real world, and an attachment to the virtual, where *"avoiding eye contact and face-to-face visibility"*[59] disinhibits people more, and could promote the opportunity to act-out, and/or say something about oneself that which would not be revealed without disinhibition. In fact, the 'mere' perception of some veil of anonymity, or of some digital shield, and however false, appears to promote disinhibition [209]. Adjacently, it has been noted that, "*[a] hallmark personality characteristic in substance abuse is impulsivity, and impulsivity is related to increased sensitivity to reward and decreased sensitivity to punishment"* [210]. Zhou and Li have recorded that *"[w]ithin neuropsychology and cognitive neuroscience, impulsivity is often equated with the term "disinhibition," and that "…inhibitory control mechanisms may be disrupted … resulting in a predisposition toward impulsive acts."* [211] For quick considerations here, it should be central to thought linkages that such disruption in the neuropsychological inhibitory controls, as mentioned, *leaves a brain in a jeopardized state,* unable to distinguish many elemental matters, such as the very state of 'cognitive compromise' itself; hence at least in one significant respect - the dissociation/the loss of time while engaged in addictive activity.

To gain comprehensive fidelity in the scope and the direction of this rising problem, and how it will likely negatively affect institutions of all sizes, shapes and missions, a better understanding of the modern workforces must be gained, to that which this author designates as workforce's *'Digital Atomicity,'*[60] or *Digitomicy (digit–o-missy).*[61] The author recognizes that *'Digital Atomicity,'* or *Digitomicy* will be of service to both direct, and to singularize a universe of ontological influencers, such as the confluence of intrinsic prerogatives and extrinsic attractors (as is the case with certain psychosocial elements), which can better characterize "human-ICT confluences" in the larger scheme of digital interactivity, all the while distinguishing the digital affinities of users, a physiognomy, if important. However, clarification must be had, and prior to proceeding that, in, or by *Digitomicy*, the author is not in any way proposing that present or future workforces be surveilled; quite the contrary. Abundant information regarding users and those services to which they are tied already exist, much of which will continue to exist, and can - as an example help enable the development of practical work-place systems, and the proper methods, which can combat unproductivity, and any prospect for information compromises, or losses. It is a necessity to mitigate risks related to the exposure/loss of sensitive information in all circumstances and situations where such care ought to be extended. There is also the need for organizations to develop more practical and more widely useful digital governance schemes, which are

[57] This term implies that, inspite of the existence of a firm "no personal Internet surfing on company time" employer policy, an employee risks disciplinary action, and chooses to engage in a prohibited activity at work. There have been instances where an employer has caught an employee "red-handed" as it were, when and where, the employee was actively engaged in non-work and time wasting personal Internet surfing at work. And, despite the existence of evidence related to the flagrant violation, the employee made attempts at deflecting blame, or denying the action. Sample Ref: Cushing, Tim; "More Federal Employees Caught Using Work Computers To Access Porn, Claim 'Boredom' Made Them Do It," techdirt, 14 August 2014 https://www.techdirt.com/articles/20140810/09552328168/more-federal-employees-caught-using-work-computers-to-access-porn-claim-boredom-made-them-do-it.shtml

[58] In: "The Matrix of the Mind: Object Relations and the Psychoanalytic Dialogue" [Ogden, Thomas H; "The Matrix of the Mind: Object Relations and the Psychoanalytic Dialogue," Rowman & Littlefield, Lanham, MD, 2004]

[59] Interactive users feel that the virtual world offers them a sense of "perceived," albeit false sense of anonymity, which deceptively emboldens parties to "act-out," or "self-reveal" as implied by Suler

[60] Merriam – Webster defines the term "Atomicity" (noun) (at·o·mic·i·ty \ at mis tē, at -, − tē, −i \) in the following way, as "the number of atoms in the molecule of an element" or as "the nature, character, or property of being atomic." Author intends the designation of *"Digital Atomicity"* or *"Digitomicy"* to be the means of identifying and representing compositional values of digital communities and users (digital foundations/digital atomics) in relation to systems and services, the character and the distinctions of users, the nature of the co-existence of users with ICT instruments and conduits, to ably represent 'human-ICT' *"amalgamation efficiency."*

[61] *Ibid*

well coordinated with emerging population habits in the digital century.

### 6.2.6 More bits and more bytes: threat foundations of our digital future

More and more people are gaining access to the Internet by each year; an anticipated reality to be sure. There are 3.4 billion Internet users (46% penetration) globally, and in the United States, mobile phone usage has climbed from 1 h a day, 5 years ago, to more than 3 h a day in 2016 [212]. The number of devices accessing the Internet has doubled in the past 5 years to 3.6 billion, and will rise again, to 4.7 billion by 2020 [213]. "In 2017, one-third of the world's population or 71.0% of all Internet users will access social media. Among those users, 60.8% are predicted to be on Facebook and 10.6% of them to be using Twitter*"* [214]. Therefore, Privacy risks and the Security risk of exposure and loss are not about to fade away. If anything, today's employers are going to be straddled with those in the workforce, who have significant workplace maladjustments in this respect. How are employers, whether they be private sector firms or public sector entities, to cope with the onslaught of workplace productivity and quality related management concerns, resulting from effects generated from our collective foothold in the Digital Century. Will *"smokestack" industry style* management models, skill-sets, working principles, techniques, protocols, and organizations serve the Digital Century and needs within? The answer is, certainly not. Yet, organizations from top-level government entities to private sector entrepreneurial tracks, and venerated industrial 'kahunas'[62] appear to not only have their immunizations not up to date for travel into the Digital Frontier, but, they also continue to pack for a tropical vacation, when the local climate is quite cool.

Under such circumstances, national level attention to the need for user education will be essential. Existing organizations of all sizes, shapes and varieties will need to change considerably, or there will be the need for new organizations - with fundamentally different structural frameworks, management schemes and support systems to ensure significantly greater accountability in all operational areas related to cost, timeliness, and quality, without which, global economies are likely to experience as yet unseen, startling shrinkages. Correspondingly, and with direct respect to Privacy and Security of personal information in the enterprise, either a sizeable augmentation and/or reinforcing of the existing, and "in the pipeline" means of affording safeguards/protections for people's Personally Identifiable Information (PII) must be made to exist. Lastly, it will perhaps become necessary in the short to mid-term, to invent and to deploy new means of protecting data, and ensuring the long-term safety and security of data uses.

### 6.2.7 Threats against privacy and security: new workplace considerations

Privacy and Security compromises routinely occur among technology users, due to many governing factors. The author wishes to remind the reader that "human error" is primarily responsible for industry security breaches/privacy breaches, and that "management of human error should be of high priority in organizations*"* [215]. "Human error" has its roots in both complicated and uncomplicated origins. Human Error is revealed both explicitly and implicitly within any organization's workers. A 'general lack' of attention to detail by workers; their inability to think logically of needed operations; an inability to understand operational methods and those means arranged specifically to achieve goals; their inability to understand consequences of deviations from the required operational processes; a general lack of proficiency with technology and its operations etc., are prime causes for human errors, which manifest and propagate. Nevertheless, what are the root-causes to Human Errors? Once again, within an organization, there are likely to be many causes: beyond the issue of poorly structured organizations; underprivileged leadership skills at the helm; inadequate indepth, interoperable, interdisciplinary and wholistic subject matter knowledge by staff, are some of the core contributors that lurk behind propagating human errors.

Three <3 > Privacy and Security vulnerability characteristics[63] that contribute to a general inability to configure organizations, having explicit aims to protect Personal Privacy and the Security of sensitive information will be provided. However, to begin, the informational stage requires to be set such that interconnections and contextuality can be made visible best.

### 6.2.8 Disruptive generational shift and the evolving privacy and security threat landscape

To those observant, it is amply clear that securing and ensuring continued Personal Privacy in any enterprise is simply not a function or task of following the act of "compliance by check-marks/check-lists." Historically, organizational staff and their collective capabilities have composed the backbone strength of any firm, their products, and their services. That criterion has fundamentally remained unchanged. However, 'Privacy' being the primary subject of discussion, the capabilities of modern workforce compositions in that respect is worthy of exploration. Restating, in the United States, Millennials have surpassed Baby Boomers within the U.S. workforce

[62] "Kahuna" \ ka·hu·na \ k - hü-n \ (Noun), *"a preeminent person or thing"* (Merriam-Webster) https://www.merriam-webster.com/dictionary/kahuna

[63] See "8.3. Righting The Perspectives on Modern Workforces"

[216]. Elsewhere too, this is fast becoming the case. Also as stated before, how, those who are doctors, nurses, teachers, judges, lawyers, carpenters, policemen, computer programmers, plumbers, contractors or spaceship builders in our communities and countries deliver services - in this case, work to assure the personal safety and the security of sensitive personal information, is for all of us to grasp, to appreciate, or to remediate as a society, if and when necessary. Beyond the challenges that this author has already noted in terms of a generational shift in the workforce, one of the most important and fundamental 'change elements' inherent to the demographic disruption in the workforce - will be a most persistent challenge, one that will plague employers and workforces, and likely for the longest. The challenge facing organizations involve the need to take key steps to prevent and/or stem any loss of "institutional memory," [217] crucial to the continuity and survival of organizations, both large and small. Such a task will be made more difficult, given the present-day quality of workforces, and the nature of development to be had [218]. Naturally, challenges are not insolvable, as solutions exist, and the solutions are certainly implementable [219]. Not unlike dealing with other generations however, there is a certain amount of wholistic discretion to be applied, to arrive to the most appropriate personnel configurations in the enterprise.

### 6.2.9 Some sector-side breach characteristics

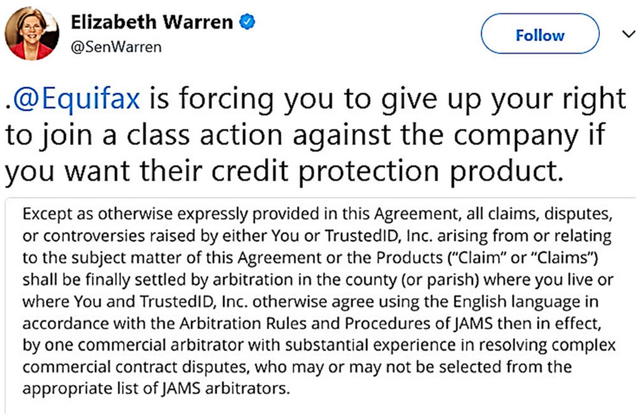
Data breaches are fast arriving to "go… no-go" points, where a single informational 'breach' could prove to be an 'extinction-level-event' [220] for a firm, costing the company, quite possibly its last breath [221]. Juniper Research forecasted that cost of data breaches would surge upwards to $2.1 trillion per year by 2019 [222]. Meanwhile, a brief broadened view of 'breach realities' on the ground should be 'mapped-out' in the following manner. Willis Towers Watson, a global consultancy, in interviewing U.S. employers discovered that 85% of those surveyed had said, 'cybersecurity was a top operational priority,' yet 53% of them lacked a formally articulated cyber-strategy [223]. Yahoo was a good example of such a problem, where, as it has been reported, 'every user account ever created' was compromised. When the problem struck, top management tried their level-best to manage and contain the news of the compromise and the 'internal toxicity' [224] it alone was responsible for creating [225], and instead of warning its subscribers/users, the company attempted to "slow-roll" the bad news [226] in increments, hobbling an Internet veteran, and an widely identified brand. In perusing results of a 'Human Element & Risk Culture Survey' from the global consultancy Willis Tower Watson (WTW), the findings may allow us to better understand compromising circumstances that arise, as it did in the case of Yahoo, a bit better. The WTW findings indicate that breached environments/companies have shown to lack *"comprehensive training especially among IT staffers, a fundamental lack of awareness of the value of customer centricity, domain-relevant knowledge and the importance of business integrity"* [227].

Still, that WTW information does not comprise the complete picture regarding the vulnerability of information systems, and in the vulnerability in protective super-structures and sub-structures too. Still, another WTW assessment of insurance data revealed that, 90% of all cyber-related insurance claims are prompted by (as stated before) some type of "human error or behavior." And, adjacently, we will want to consider that IBM' security research has determined that "60% of all cyberattacks are carried out by insiders and three-quarters (3/4) of those involve malicious intent, while one-quarter (1/4) is attributable to inadvertent actors*"* [228]. And 56% and 54% of IT professionals in the U.S. and UK respectively identify disgruntled employees as those that could deliberately compromise systems and steal customer/client data.[64] These "indicators" designate the message clearly that, where protection of informational assets in an organization is concerned, employers worldwide (whomever they are), need to secure "appropriate people" who possess "appropriate qualities and skills" for the task. For example, conscientious Healthcare employers should certainly avoid a certain sort of candidate who is surely not well configured to work within a healthcare environment, and its many demands [229].

## 7 Examples of varied pathologies in that "breachable" ecosystem

Somewhere between the month of May and July of 2017, one of the largest credit reporting companies in the world was electronically penetrated by parties yet unknown. It is not likely to be confirmed, when exactly the penetration happened, and naturally then, if it happened between May and July of 2017. What is known however, is the following. Equifax did claim that personal details [230] of approximately 143 million Americans have been compromised. It is also known that senior executives of the company sold a certain percentage of their personal holdings in the company [231], before the breach was announced (a good reflection of the company's overall commitment to fiduciary responsibility). Finally, Equifax offered free credit monitoring and identify theft protection service, with a catch; if you decided to accept Equifax services, you had to give-up the right to seek redress from the company (See Fig. 21). After a public tongue-lashing, Equifax stated that their indemnification statement would not apply to this incident. How is any or all of this possible in our time? Should not, the likes

[64] "Decoding Cyber Risks: Willis Tower Watson Cyber Risk Survey," US & UK Results, 2017



Elizabeth Warren
@SenWarren

.@Equifax is forcing you to give up your right to join a class action against the company if you want their credit protection product.

Except as otherwise expressly provided in this Agreement, all claims, disputes, or controversies raised by either You or TrustedID, Inc. arising from or relating to the subject matter of this Agreement or the Products ("Claim" or "Claims") shall be finally settled by arbitration in the county (or parish) where you live or where You and TrustedID, Inc. otherwise agree using the English language in accordance with the Arbitration Rules and Procedures of JAMS then in effect, by one commercial arbitrator with substantial experience in resolving complex commercial contract disputes, who may or may not be selected from the appropriate list of JAMS arbitrators.

**Fig. 21** A Portion of the Twitter Posting by U.S. Senator Elizabeth Warren, Regarding Equifax's Protective Offering Upon Credit Information Breach. Source: Official Twitter Account of U.S. Sen. Warren

of Credit Reporting Bureaus be temples, sanctuaries, for sensitive information? The reality is, no entity has demonstrated it can claim assuredly to be "safe," for any of your valuable information to be housed within. When the reader completes this reading, and comprehensively, the universal malignancy and menace related to informational insecurity will perhaps be better revealed in terms of Personal Privacy.

At the time of this writing, 'The Guardian' newspaper was reporting that one of the "big four" accountancy firms Deloitte, was targeted by malicious intenders, and was penetrated, which resulted in the exposure of private and confidential data belonging to their "blue-chip" clients [232]. Deloitte, a leading global Risk Management entity, predictably, and in-line with the running industry trend, had not noticed the infrastructure and data compromise for months [233]. How is it possible, that one of the world's largest accountancy and consulting companies with a global footprint, while handling agglomerations of sensitive documents belonging to individuals, or governments, and everything in between, suffer a compromise at all; especially since, the consultancy also houses a Risk Management business? ISACA (founded as the Information Systems Audit and Control Association)[65] has some answers for us in this regard. First, in a global study of 461 cybersecurity managers and practitioners ISACA found that ~25% of all those that were primarily responsible for security in their organizations, were entirely unaware, if their corporate infrastructures were compromised [234]. Year after year, security personnel remain unaware of breaches. In this regard, ISACA offers that, *"the large number of individuals who do not know if their enterprise had been breached…"* despite important advances in cyber-security approaches, means, there is *"…a broader systemic problem"* [235]. These systemic matters constitute the full universe to which all must present full attention, as the information regarding these and other adjacent matters grows dire and direr. Let us consider the following matter. The General Data Protection Regulation (GDPR) in the EU was considered[66] the greatest sea change in the area of Privacy. Surely, the GDPR will significantly alter the face of Privacy from both, theoretical and practical points of views. Undoubtedly, GDPR mandates practical changes to Privacy related considerations and in the way protective processes, procedures and systems are emplaced and run. All EU member states will need to enforce the General Data Protection Regulation very soon. Each, and every entity in the EU that has, and/or will handle sensitive data of European Union citizens will need to abide by the many aspects of GDPR. So too will non-EU countries, and those entities within the respective borders of non-EU countries that have, or will have economic and trade relations with the EU, or their counterparts in the EU. The following study will be of good interest, at least in terms of the enforcement related issues, and the liabilities that could arise in terms of GDPR non-compliance.

In an assessment performed by Vanson Bourne and commissioned by McAfee that involved 800 senior global business professionals in relation to GDPR enforcement, only 47% were confident of fully knowing where (in the world) their data was stored/located, and only 2% of management personnel on the whole said they understood relevant Data Protection regulations as applied to their specific organizations [236]. Reading such a statement, we are forced to have to ask, who, and how anyone can "protect assets," when the location of those assets are unknown – even for a second. In addition to the McAfee assessment, the following ISACA determinations should also be studied in terms of the systems yet to be configured, to protect both information and systems.

ISACA candidly admits that most organizations having open cybersecurity positions fully expect them to remain vacant for extended periods, as most candidates presenting themselves for employment in the field these days are unqualified [237]. The organization, having performed an 'Enterprise Privacy Function,' review among the organization's global membership of Privacy and Risk professionals additionally learned that less than one-third of the Professionals are very confident in their own Enterprise's ability to ensure the privacy of sensitive data [238]. Contiguously, more than half of those ISACA Privacy Professionals studied - do not think that consumers today should feel confident that enterprises are adequately protecting their personal information [239]. As this author has asked previously, should none among us ask, *why, the 'experts and professionals' who are being paid to secure highly sensitive personal information 'in the belly' of their respective companies are "not confident" in the very mechanics and machinery they imagined,*

[65] ISACA identifies itself as "the world's leading independent, nonprofit association in governing, managing and assuring trust in an evolving digital world."

[66] Until the historic Supreme Court's Privacy ruling in the Republic of India

*conceived, developed, deployed, and now maintain; the very same mechanics and machinery, we are imperiously instructed from time-to-time by entities (both public and private) as "needing to exist" – to protect us from the loss of our most sensitive and private information?* [240]

ISACA's candor in the matter is to be commended. With respect to the industry as a whole, much more remains to be done.

## 8 Some examples of the threat ecology working against privacy and security

Susceptibility of persons, to informational compromise, to surveillance etc., has been discussed herein, to the extent that it must be, to provide the reader an adequate coverage generally warranted to allow comprehension of just how the interoperability of vital "individual attributes" matter to fittingly 'structure' knowledge-workers into organizations, and directing missions. There are many sides to susceptibility, such as the psychographic contours and/or features of the informational and personnel ecosystem, as in the systems of planning and instrumentations related to the execution of organization objectives in any operational ecosystem. As an extension and representation of this aspect, consider that 58% of information infrastructure attacks in the Financial sector, and 71% in the Healthcare sector, originated from the inside [241]. On face value at least, it appears the Healthcare sector is more susceptible to informational compromises from insiders, than the Financial sector. So, why are insider attacks higher in the Healthcare sector?

Another important consideration of a vastly different character and shape is that 64% of Americans are agreeable to paying a data extortionist's demands, whereas, globally (except U.S.), only 34% are agreeable to the same [242]. A study involving U.S. consumers, small, medium, and large-scale enterprises have Americans being ~ 60 agreeable to paying a data ransom [243]. Notwithstanding the existence of any system or practice vulnerabilities, it is readily deducible that U.S. operators will be more susceptible to data extortionists by way of their agreeability to pay data-ransoms. Another informative and highly connected piece of this puzzle is the state of U.S. Small and Medium sized Enterprises (SME)/Small & Medium-Sized Businesses (SMB) to be able to repel 'victimization' by a data extortionist. Ponder for a moment that, at a time when 1 in 131 emails dispatched are malicious (the highest rate in five years) [244], only 33% of all SMBs feel that they have the capability to 'detect and block' attempts to penetrate their respective information infrastructures, while 69% of all SMBs have neither the institutional budget, nor the internal expertise to lay down any measure of defense, or the protective cover against attempted infrastructural compromise [245].

The last element of susceptibility shared in this section will be the multiple aspects of susceptibility of the modern knowledge-worker in relation to global business needs. Composing highly productive workforces and organizing their skill-sets to be practitionally sensitive to data protection and personal privacy demands - is not a trivial task. Once again, it is necessary to reflect upon the generational shift in workforces, and the preparatory steps employers will have to take to adequately qualify, and to make exist those suitable mechanisms for institutional protections more universally, and to have all specific and sufficient indemnities as necessary.

### 8.1 Nature of susceptibility and the enterprise's first line of defense

Data protection to result in Personal Privacy and the Security of personal information is ultimately the product of engineered convergence of many technical, organizational and managerial foundations; foundations associated to Access Controls, Data Validation, Data Verification, Data Integrity, Rights Management, Data Classification, Data Storage/Re-Use/Distribution, Data Manipulation Tools & Services, Protective Services Foundations (such as Encryption) etc. There is so much more to all of this, than meets the eye, or the ear. The engineering of the convergence of foundations - is most often left in the hands of those that are not sensitive enough to threats, not situationally aware, not professionally knowledgeable (as it has been shown) or perceptively attentive – to be sufficient, efficient or effective, in actions that must be taken to protect Personal Privacy and Security.

Symbolically at least, the challenge of staff composition needs in organizations and the engineering of the aforementioned convergences of the many foundations are, in a conservative estimation, at least correspondingly as large a challenge as T.E. Lawrence's need for crossing the Nafud (Al-Nafud) Desert; a challenge that needs undertaking, and completing. In Lawrence's case at least, we know that that the Arab forces that he had advised and had assisted to mold, defeated the Ottoman forces at Aqaba. Here, on the other hand, we know not, what prospects hold for employers faced with the demand of needing to organize and shape a superior informationally secure enterprise. Let us look at a few broad-spectrum problem points relating to personnel that information rich environments will have to overcome in order to be better protectors of Personal Privacy and Personal Security.

### 8.2 On righting the next generation human resource pool

'Human Resources' and 'Management' literature seem to have at least fashionable interests in the Millennial generation's entry into the workforces, imposing "mega-shifts" to the organizational edifices and core, intended to have companies remain engaged and relevant in the market – well into the future. Most of the available literature in this regard is U.S. centered and lack great empirical fidelity. Judging by the information that is available, it is easily determinable that workforce transitions are not going to be pain-free. The implications visible through the information available shows implications that are global in nature. As new employees, when millennials stream-in to the core of today's enterprises, those large-scale structural and operational adjustments that were needed to have been placed into service - to ease and expedite a productive initial co-mingling of the new and the old workforces, and the subsequent co-existence of inter-generational transitioning workforces will not have been in place. Management and staff will have largely been caught "flat-footed" in their inter-generational workforce transitioning preparations.

Yet, in the midst of all workforce mingling and adjustments that is needed, wheels of government, finance, of commerce, industry etc., must keep churning, being productive, being efficient, and being effective. For instance, the task of preserving and maintaining Personal Privacy and Security of persons cannot stop, nor can it be interrupted while adjustments in the workforces are being made, when training is being carried out, or during any mending of unfortunate organizational hitches, or a glitches. The main employer objective regarding the highlighted staff adjustments necessary is, to circumvent business/operations/market disruption as a consequence of said staff adjustments. Unfortunately, for those who are seeking specific wisdom in such matters, from oracles of Human Resources, and/or Management Consultants and Organizational Specialists etc., in relation to Millennials, their presence and integration into workforces, performance metrics etc., the empirical evidence is scant, eventhough there is good interest in Millennials becoming the dominant workforce. Therefore, organizations find the need to muddling through, as operably able. Herein are few diagnostic entries, included here for their broad-stroke relevance to the composition of renewed workforces that would be able to support and to maintain Personal Privacy and Security demands.

### 8.3 Righting the perspectives on modern workforces

All-purpose characterizations and discussions of Millennials regarding denote them being volunteer minded/community oriented, being purposeful, caring, and politically engaged. The one empirical study (as it has been possible) in particular, worthy of greater inspection, dissection and analysis, originates from Psychologist Jean Twenge. Twenge and her colleagues in *"Generational Differences in Work Values: Leisure and Extrinsic Values Increasing, Social and Intrinsic Values Decreasing,"* largely dismiss common claims of generosity and concern expressed for their fellow-man by Millennials. Twenge and colleagues have determined that Millennials are more concerted on achieving extrinsic goals,[67] than intrinsic goals,[68] and that there is less Millennial' concern for others, and for civic duty, as noted commonly. As a side note, as it was recorded last by the U.S. Bureau of Labor Statistics, millennials had the lowest national volunteering record, at 18.4%.[69] Another key aspect of personnel characteristic that employers need to concern themselves with is that quality of the employee to be able to apply personal and professional skills to fulfill employer's mission-centered objectives.

In relation to aforementioned points, results from the *"Wave 2 National Epidemiologic Survey"* of the *"Prevalence, Correlates, Disability, and Comorbidity of DSM-IV Narcissistic Personality Disorder"* [246] will need to be analyzed contextually. This comprehensive national (U.S.) analysis enunciated affirmatively that Narcissistic Personality Disorder (NPD) *"is a prevalent PD (Personality Disorder) in the general U.S. population."* How prevalent? The study had discovered that people in their 20s, suffered Narcissistic Personality Disorder nearly **3×** more than those over the age of 65 [247]. In a meta-analysis of American college students who undertook the Narcissistic Personality Inventory (NPI) examination between 1979 and 2006 showed almost two-thirds of the more recent college students demonstrating a 30% increase in narcissism scores [248]. In *"Narcissism Epidemic: Living in the Age of Entitlement,"* [249] the authors identify modern day narcissists as those people who, "strive to create a "personal brand" (also called "self-branding"), packaging themselves like a product to be sold."

Why should we discuss Personality Disorders? Personality Disorders are hard to sense, detect, and most importantly, confirm. The author has broadly, but briefly, introduced the reader to insider threats, and consequences. *Narcissism* and *Impulsivity* are closely connected [250]. Moreover, the presence of narcissism would certainly prevent a candidate from adequately interfacing with the enterprise and its many segments properly. Moreover, an employer's gamble - that narcissism could not/will not spawn a series of informational compromises having already presented certain psychosocial characterizations herein, is a risk that simply cannot be taken.

[67] "Extrinsic work values focus on the consequences or outcomes of work—the tangible rewards external to the individual, such as income, advancement opportunities, and status." [Twenge et al.]

[68] "[I]ntrinsic work values focus on the process of work—the intangible rewards that reflect the inherent interest in the work, the learning potential, and the opportunity to be creative." [Twenge et al.]

[69] Bureau of Labor Statistics, U.S. Dept. of Commerce, [2015], February 2016

The millennial workforce entrant is forced to have to comingle with people of other generations already within the enterprise. While millennials are considered to be 'social beings,' they are not so - in the social norms sense; they are 'virtually social;' where societal norms governing human connections and relationships are not correspondingly the same, as they are in the real world. When millennials comingle, and interface with the existing workforce, there are no guarantees in advance that there will be any acceptance of millennials at all by other generations in the workforce mix. Some are likely to "fit-in" while others remain on the margins, never integrating into the whole as part of a larger team [251]. An even larger organizational issue of concern, that is likely to cause significant clashes[70] in the workplace involve people's roles and their work-values, as in their 'presence,' 'communications,' 'accountability,' 'production,' 'output quality,' 'diligence,' 'sense of commitment' etc., between generations. All such considerations are important when organizing to safeguard and secure Personal Privacy and Security of informational enterprises. When values are not aligned, conflict emerges, and dissynchrony propagates throughout the establishment, resulting in significant failure modes [252]. Consider, if one is prone to be afflicted by *NOMOPHOBIA, PIU (Problematic Internet Use), IGD (Internet Gaming Disorder), Internet Addiction Disorder (IAD) or FOMO (Fear Of Missing Out),*[71] and to also prone to checking their mobile device ~ 150 times in a day, or ~ 6.5 times every hour[72] how will it be possible for the *"umbilicalized worker"*[73] to be part of a larger enterprise team, more institutionally engaged, and more mission-centered? If a worker is disconnected from institutional needs, mission-centricity and is constantly prone to be interrupted by Social Media activity, and disturbances from family, friends, or others how is such a party to integrate with the whole that is more institutionally centered, and focused upon achieving missions? Who precisely will be the responsible party to the human errors/process errors that such a person will likely introduce into 'mission-flows' that has the potential to weaken or destroy mission-centricity? The reader is reminded that *"[n]arcissism was found to be positively related to Millennials' reported belief that others are interested in what they are doing and the desire for others to know what they are doing"* [253]. Also, that "*[t]he online environment allows narcissists to effectively manage their image by controlling the information and activities that are displayed. This control allows narcissists to hide their inadequacies and, thus, bolster their self-esteem."* [254] All of this simply means, employers must be devoted to mission-centricity more, and hold employees accountable to the performance of assigned tasks as required, in this case, to those duties that are related to the protection and preservation of people's Privacy, and their Security.

Three <3 > characteristics associated with the millennial workforce that should be part of all important considerations relating to protection and preservation of Privacy and Security specifically concerns that generations' potentiality to meet performance expectations in the workplace. First is the matter of "Engagement." Broadly, elements of engagement can provide steady insight into some key aspects of labor affairs. The research arm of the Gallup organization performed engagement analyses upon the Millennial generation, their presence, and their performance in today's workforce. Gallup revealed that only 29% of all Millennials are connected to their work, are engaged, and are delivering for their employers, while 71% are "disconnected" and are "disengaged" from their commitments to their employers [255]. Disturbingly, Gallup stressed that 16% of the 71% are directed to do 'damage to the companies' in which they are employed [256]. Gallup finds that *"[t]he millennial workforce is predominantly "checked out" — not putting energy or passion into their jobs"* and that *"[t]hey are indifferent about work and show up just to put in their hour,"* costing the U.S. economy at present, **US$ 30** billion/yr. in turnover costs [257].

The Second characteristic of concern regarding the millennial generation involves their use and command of information technology – a double-edged sword. On one side of the sword, millennials are reported as being enthusiastic tech-users. Inspite of their reported enthusiasm for information technology and its use, they are criticized often for not being conscientious of technology related security demands. Technology industry channels quite often reports on this subject, albeit wrongly [258]. On the other side of the sword, is the often-reported broad falsehood that millennials are "tech savvy." The desire, and a general inclination to use technologies in no way substantiates proficiency, nor is technology use by millennials (or frankly, one from any generation), any evidence of working knowledge of the many aspects of technology, or of the insides of those aspects. This author's experience in government and industry is that millennials are predisposed to liking technology use, but their skills

[70] These thoughts are offered strictly in the context of Millennials entering/engaging/overlapping inter-generational workforces as part of a larger organizational need to make allowances for workforce transition needs. In the matter of total workforce replacement, or the initiation of longer-term HR activities, management systems and organizational structures will need to be altered and new templates will need to be deployed to manage personnel and direct productivity

[71] See section "6.2.4. Psychosocial Characterizations of the Digital Workforce In Relation to Informational Access & Use," for a more detailed examination

[72] See section "6.2.3 Frequency of Access to Digital Devices, Interruptions, and Productivity Losses at Work," for a more detailed examination

[73] Author is making a humorous reference to a worker receiving all of his 'neural nutrition,' 'thought directions' and 'action directions' through his digital device(s), serving as umbilical cord(s) to an amorphous digital cloud, a 'celestiality,' where all "zeros" and "ones" go to claim residence – far distant, and much apart from the human race

associated with technologies and their proficiencies in and of technologies are not universal, not unlike those from other generations. That which is a generally acknowledged problem among employers with larger numbers of Millennial staff is that there is a general reticence by Millennial employees to follow instituted safety and security policies. Evidence that is more empirical is warranted - to understand precisely the reasons for safety and security policy violations by the Millennials. Anecdotal evidence points to a general sense of invincibility, dislike for authority, dislike for procedures and processes, short-attention span, failure to be able to think analytically and judiciously, failure to comprehend fully - the consequences and/or repercussions, general insensibilities lending to being unable to understand rules function etc. If some, many, or all of these characteristics are present among workforces to whom responsibilities to protect sensitive information are entrusted, the likelihood that aims to protect the safety and security of private information will be negatively affected - will remain high.

The Third characteristic of a Millennial generational concern is their level of preparation to enter the workforces. At least, in the United States, over the last century, public educational systems have been machined into a corn-fed parasitic leviathan, primarily existing to serve itself, and the bureaucratic elements within [259]. 74% of students questioned believe their college/university is failing them when it comes to job preparation.[74] In a survey of 500 Senior U.S. Executives by Aberdeen, 92% of them declared that American workers are not as skilled as they need to be, and 59% of them blamed the education system for the gap in U.S. Worker skills, while 64% of them were of the assessment that due to the lack of properly skilled U.S. workforce, there will be less investment in U.S. firms in the overall.[75] In another survey by Aberdeen,[76] of more than 500 C-Suite Executives globally, 80% of all employers believed that the ‘skills gap,’ that gap between much needed skills, and those skills that are presented by employee candidates in the market - is real, and 76% of all organizations were using contingent labor to enhance their workforce and close talent gaps [260].

Regarding technology use, the mere ability to interface with and to use technology - does not mean, nor should it be strangely correlated to proficiency. The same can be said for education. To have been commissioned at a college or a university infers neither mastery nor proficiency in any subject. Historically, in the United States, *grade inflation*[77] has ‘glued-on,’ the veneer of college preparedness, when there is an overall lack of competence [261]. More and more, *the underpowered*[78] *and over-confident college graduate covets to be part of the “skills economy” without skills, and fancy to be part of a “knowledge economy,” without knowledge.*

In a “Workforce-Skills Preparedness Report” by human resources firm “PayScale Human Capital,” for instance, 87% of recent graduates had a self-appraisal that they were prepared for their job, while only 50% of their managers had similar confidence. The recent graduate and prospective employees is largely suffering from severe deficiency of skills crucial to the workplace. 60% of all hiring managers stated that recent graduates/applicants lacked “critical thinking/problem solving” abilities, while 56% of all hiring managers said that applicants lacked “attention to detail,” and 46% of the managers stated that applicants lacked “communication skills,” and 44% said applicants lacked the skills to establish maintain “ownership/accountability.”

Looking forward, the overall capabilities of institutions to protect people’s Personal Privacy and Security, and the large-scale workforce’ generational transitions underway, the over-confident estimations of technology comfortability and savviness of the millennial generation will need to be better examined. For a U.S. perspective on this, and how it might apply to parts of the world elsewhere, the author has chosen to rely upon the work of the ETS Center for Research on Human Capital and Education. In a report that uses Program for the International Assessment of Adult Competencies (PIAAC) data, and one that is uniquely focused upon millennials, *“America’s Skills Challenge: Millennials and the Future,”* the knowledge and skill-sets of U.S. millennials are compared for the first time to their international peers. The findings wipe off the superficially artisan, cheery, defective, and dubious ‘reporting’ that grace the opinion pages, describing how effectively U.S. education is competitively preparing tomorrow’s workforces. The authors of the said report present that the ‘singularly important message’ emerging from the report is that, *“despite having the highest levels of educational attainment of any previous American generation, these young adults on average demonstrate relatively weak skills in literacy, numeracy, and problem solving in technology-rich environments compared to their international peers.”* As it has also come to be known, “*[e]qually troubling is that these findings represent a decrease in literacy and numeracy skills for U.S. adults when compared with results from previous adult surveys.”*

The report has uncovered that, “[i]n literacy, U.S. millennials scored lower than 15 of the 22 participating countries. Only millennials in Spain and Italy had lower scores.” “In

[74] “Workforce Management” Survey, Adecco-Aberdeen, 2017

[75] “State of the Economy Survey,” Adecco-Aberdeen, 2017

[76] Commissioned by Adecco

[77] “Grade Inflation” \ noun \ Education \ *“the awarding of higher grades than students deserve either to maintain a school’s academic reputation or as a result of diminished teacher expectations,”* Dictionary.com http://www.dictionary.com/browse/grade-inflation

[78] U.S. Millennials were adequately compared with many of their peers internationally, that examination, and findings related to their levels of overall preparation will follow

numeracy, U.S. millennials ranked last, along with Italy and Spain." And this is where the findings get even more interesting, in Problem Solving in Technology-Rich Environments (PS-TRE), *"U.S. millennials also ranked last, along with the Slovak Republic, Ireland, and Poland."* Remarkably, the report states, the *"[t]op-scoring U.S. millennials (those at the 90th percentile) scored lower than top-scoring millennials in 15 of the 22 participating countries, and only scored higher than their peers in Spain."* And, "[l]ow-scoring U.S. millennials (those at the 10th percentile) ranked last along with Italy and England/Northern Ireland and scored lower than millennials in 19 participating countries." This represents a broad view of the landscape as it relates to workforce preparation for the Digital Century; more specifically, to that ability to be able to protect and defend Personal Privacy and the Security of informational enterprises.

These findings should ring alarm-bells in the mind of modern day employers who must now make significant institutional adjustments to satisfy legal responsibilities related to the protection and preservation of Personal Privacy and Security of information. Such is also 'the' "composed nature" of workforce's surveillance susceptibility, and the ways in which interconnections, and interdependence among people, processes and technology will go on to affect the ways Personal Privacy and Security of information will/can be assured.

## 9 Conclusion

Two intellectual branch offenses are routinely committed against populations with respect to Personal Privacy. One routine offense is of a psychological nature, and the other, sociological [262]. Psychologically, we are instructed by those all-knowing, that 'some amount' of liberties must be forfeited for the sake of safety and security, as it is "essential" for the larger good [263]. Sociologically, we are instructed that in increasing security measures, we become safer, and that any consequential erosion in "Personal Privacy" (for instance) is being adequately compensated, by added security measures [264]. As if situations surrounding Privacy are not hard-enough to parse already, Privacy learners also have to routinely content with security "apologists" and "false prophets" of Privacy, who, apart from being responsible for other types of violations (concepts, language – its syntactics, pragmatics, semantics etc.), continue to attempt their hand at presenting the aforementioned psychological and sociological propositions. It is for such reasons that this editorial has been written, to service the reader with a more comprehensive informational arrangement, that will likely materialize a broader, relevant, timely, intellectually fuller, and more clarified perspective on Personal Privacy and Security.

Privacy desperately needs a common language and a universal frame of reference, as in many areas of the world (including the most developed), there are strong desires to subjugate fundamental human rights in the name of security. Within this editorial, the author has attempted to provide a logical, agreeable, and durable proposition for our most basic Privacy consideration and discussion orientations, referenced around the Universal Declaration of Human Rights (UDHR). Personal Privacy and Personal Security are values that are broadly treasured by humanity. However, man is chiefly responsible for the compromise of both, as in other things.

Human "error" is the biggest culprit. Although the use of the word "error," given the range of human misconceptions, ill-adjustment, maladjustment, disorganization, corruption, and sordid unethical and unequivocally immoral behavior sets that may/could be involved, is severely unfitting. In a very broad sense, this editorial wholly concerns itself with society's preparedness (rather, the lack of it), to protect and defend Personal Privacy and Security going forward. Consider India as an example, in part, an ancient land and cradle to human civilizations. Its Supreme Court has ruled that Privacy is a constitutionally protected right for nearly 1.4 billion people of planet Earth and citizens of India. Yet, India is a country that is, in this author's estimation, the least prepared to make Privacy (now a legally protected constitutional right) realistically applicable in society, and make it viable for the long-term for all Indians, given the present day national directions, as they have been shown herein. The *Aadhaar*, known as the world's largest biometric identity program, and its nationwide implementation is an example of how incredibly ill prepared (tactically and strategically) the Indian economic, political and social ecosystems are especially situated to fully enter and to inter-operate within a digital century. On the other hand, in the case of Rwanda, from known information, the country is organizing and orchestrating to provide Privacy protections for all in Rwanda eventhough the country's constitution does not enshrine Privacy as a basic right for citizens. In both of these country situations, it remains to be seen still, just how protected their respective citizens will be - in time.

Meanwhile, this editorial has aimed to provide a broad-stroke layout of possible failure modes in the human dimension in relation to activities mounted with intentions and designs to protect Personal Privacy and the Security of information for the immediate, and many, many approaching years. Herein, several "un-fused" aspects of Privacy not intuitively considered, as in our individual behaviors when interacting with digital tools and services, emplacement of those behaviors in organizations, struggles experienced by some in evolving national and cultural identities, and human preparations to face demands of evolving and integrating technologies, economies, systems of governance and peoples have been reflected upon. In this conclusion, the value of Personal Privacy and Security related 'self-awareness' and the now inordinate need for higher states of global self-preparedness for the protection of personal rights, and to the defence against encroachments upon the same, is briefly highlighted and discussed.

In section "3.3. The Case of Guatemala: Where The Once Oppressed – Gamely Facilitated Brutality," the role of technology supplier Tadiran was discussed, as having aided the establishment of a surveillance society in Guatemala. In El Salvador, the same equipment that was supplied by Tadiran to Guatemalan officials was used to catalog people in a different way. Author Jane Hunter, in "Israeli Foreign Policy," described that, El Salvadorian Police blocked-off many parts of the nation's downtown areas from time to time, and set-up police checkpoints, where information from ID's of all who passed through these checkpoints were routinely harvested and analyzed with technology provided by Tadiran. From the harvested information, the Police analyzed the travel patterns of all the people. According to Hunter, if the Police determined that a person was in an area, where and when "he was not supposed to be," that right away made the person a suspect [265].

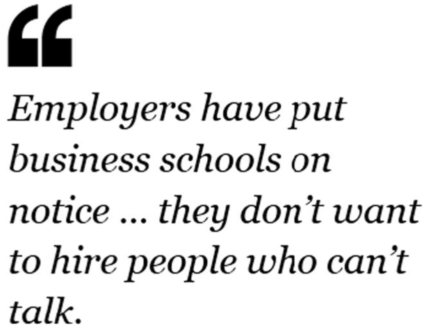
In the here and now, in New York City, according to the New York Civil Liberties Union (NYCLU), New Yorkers have been subjected to such a type of "stop-and-frisk" by police authorities, **4** million times since 2002, where nearly 9 out of 10 'stopped-and-frisked' New Yorkers have been completely innocent. NYCLU notes that Black and Latino communities continue to be the majority target of these New York City police tactics overwhelmingly. Meanwhile, in one of the many thousands of such instances, an innocent bystander Hadiyah Charles was arrested by New York City Police for filming a "stop and frisk" encounter. The New York Civil Liberties Union (NYCLU) reported Charles was shoved by NYC Policemen, who proceeded to subsequently handcuff her, arrest her, and hold her in a jail cell for 80 min for video-recording the event. A lawsuit filed in U.S. Federal District Court [266] by Charles, against the New York City Police Department, the Chief of Police, and several Police personnel has been settled. But, why discuss Police? Police are discussed due to the nature of Charles's encounter with an agent of the government, also because the agent is one that is authorized to maintain law and order. We also discuss Police Agencies and members of their forces in this conclusion because they have the power to use force – force to confront, force that imposes upon a person a certain exigence – able to breach one's personal civil/constitutional privileges (perhaps involuntarily), force to question, cordon, detain, arrest, and to discharge deadly-force. In many ways, the qualifying temper and dispositions of 'Police-Public' encounters in many ways define the strength of civil society and its structures. Within the discussions herein, and to this conclusion, an encounter with Police as Charles did, begins to outline and describe for us - the background, design, structure, and composition of protective ecosystems, and those remedies to be put into place to strengthen and assure protections in those ecosystems. With specific regard to Personal Privacy and Security for instance, we must pose if Police routinely detain, question and/or search public without any "reasonable suspicion," or the existence of warrants issued, or as in the case of Charles, plainly interfere and impede in constitutionally protected activities, and or otherwise engage in unlawful arrests and detentions of law-abiding citizens.

Lack of transparency into Police forces and their activities for instance, has historically precluded the conduct of research on effective Policing - more generally. For example, in the U.S., no comprehensive statistics exists on problems relating to Police integrity, and furthermore, no government entity gathers and represents data adequately, related to criminal arrests of Policemen and women. However, in a recent groundbreaking study of law enforcement entities in the U.S., performed with support from the U.S. Dept. of Justice, uncovered that of all criminal arrests made of Policemen and women in the U.S., **54%** of the total were serious enough to warrant dismissal and separation from the Police forces [267]. Police agencies are merely a reflection of the communities, and the people within the communities they serve. It is said that the problem with Police Departments are no different from those that are experienced by corporations, universities, labor unions, and government agencies [268]. David Dorfman disclosed that one known and indelible aspect of Police operations is that, "Police lying is no "little secret."" [269] Dorfman adds that corrosively, Juries are thoroughly capable of overlooking, completely ignoring, or side-stepping the fact that Police testimony can in fact be, *"unbelievable, unreliable, and even mendacious,"* that "[j]udges, prosecutors and defense attorneys report that police perjury is common-place,' and… police officers… concede that lying is a regular feature of the life of a cop." [270]

Regarding "search and seizure" activities by Police in particular, examining Melanie Wilson's thoughts in *"An Exclusionary Rule for Police Lies"* will be prudent with respect to discussion of Personal Privacy and Security. Wilson tells us that, "[e]ach police lie that manufactures a reason to support an otherwise "unreasonable" search or seizure deprives all citizens of their confidence in the [U.S.] Fourth Amendment's protections against government intrusions into privacy, liberty, and dignity*"* [271]. Regardless of where we live, all actions taken by those such as the Police, in violation of constitutionally granted privileges, erode the very stability of our societies. A landmark "abuse of Police authority" study performed in the U.S., has determined that "[t]he potential abuse and actual abuse of Police authority remain both a central problem for Police agencies and a central public policy concern*”* [272]. This simply intimates that the risk/chance of “Police-Public” encounters ending poorly will continue to be high. The study found the following particulars relating to Police Departments, and Police Personnel cultures.[79] The same particulars can be judged contributing to the persistence of poor “Police-Public” encounter outcomes. Findings showed that 67.4% of all Police personnel either agreed or strongly agreed that if one policeman/woman reported another’s misconduct, s/he would likely be given the “cold shoulder” by others. 52.4% of all Police personnel either agreed or strongly agreed that it is not unusual for one member of the police force to “turn a blind eye” to improper conduct by another, or others. Moreover, 61% of all those who were studied either agreed or strongly agreed that they do not always ‘report serious violations involving abuse of authority’ by fellow Police personnel. None should be surprised at the number of formal complaints filed against members of the New York City Police force, where police personnel have come into contact with the public, and verbal threats, physical interference and intimidation as tactics were used to stop the public from recording Police’ interactions with public.

Due to the number of those types of cases, the New York City Police had to send a “reminder”[80] to all among its roll (message to New York’s Police force, see Fig. 22), to be mindful of U.S. constitutional privileges of a Citizen, which the Police are not to violate, when a civilian is seen recording ‘Police-Public’ encounters. A list of at least 2 dozen lawsuits have been filed against the City of New York,[81] since that “reminder” was dispatched [273], which indicates at the very least, a ‘reading and comprehension’ problem among members of the New York City Police force (see Fig. 23).

As this editorial has been discussing, this issue of ‘Police-Public’ encounters is related to Personal Privacy and Personal Security, as any action by a Police force, to stop, detain and question members of the public has to be synchronous with the principles of the Universal Declaration of Human Rights – being a basic instrument that supports the existence of civil societies. Respect for human dignity, and respect for the law, are not mutually exclusive principles or conditions. In this instance, subjugation of constitutionally privileged rights by Police represents an unacceptable, reprehensible, and roguish act in the least, especially when members of the Police force care to (as they so often do) announce themselves as a group of professionals who are responsible for the “enforcement of laws.” To be clear, while discussing this very American issue, none should construe that this discussion item could not be of interest to the rest of the world; it surely is. And naturally, the type of NYC Police behavior being discussed is not unique to New York City. The behavior of certain Indian Police officers have been discussed herein too, where staff from the local Police Dept., had stood-by as spectators, while a crazed mob, beat a man to death.



“

*Employers have put business schools on notice ... they don’t want to hire people who can’t talk.*

**Fig. 22** The Crucial Skill New Hires Lack. Source: The BBC - 29 August 2013

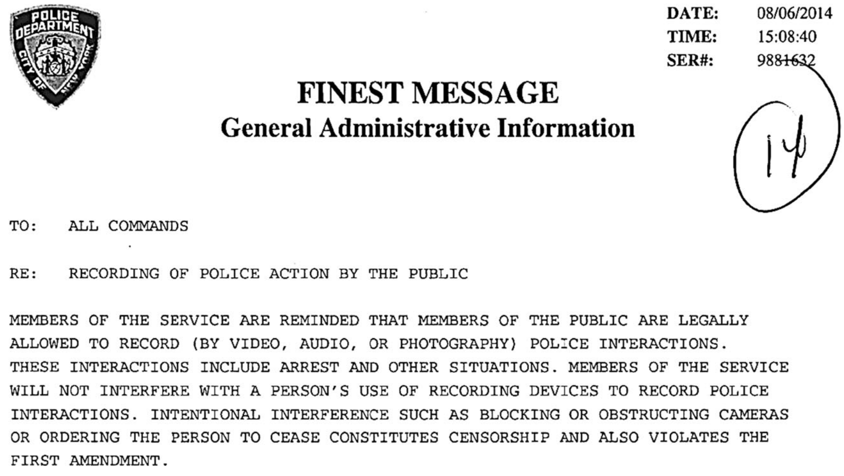
With respect to the “stop and frisk” actions of the New York City Police Department, on 12 August 2013, United States District Court Judge Shira A. Scheindlin of the Southern District of New York, determined that the constitutionally protected rights of the plaintiffs who brought a class action lawsuit against the City of New York, in “stop and frisk,” had been violated [274]. Judge Scheindlin ruled that the City of New York had been employing a *“policy of indirect racial profiling”* all along, and that the Police department *“must have individualized, reasonable suspicion that the person stopped has committed, is committing, or is about to commit a crime”* [275] Looking at this from a Personal Privacy and Security point of view, all the “stopping,” and “frisking” of ordinary citizens, had violated their Personal Privacy and Security. The important question to ask at this point is, why did it take more than a decade to get this ruling? Were there not enough courtrooms; judges; lawyers, bright minds and insights to map relevant points regarding violations and arguments, or was this simply a case of constitutional “foot-dragging,” “balanced” against politicized cries for “security”?

The author wishes to additionally remind the reader – in case it is not readily obvious, that, the following

[79] *“Too often, there is a disconnect between policies and practices, a failure of police management to monitor behavior and to respond appropriately. If police leadership does not assume an aggressive role in ensuring that the police culture is one of integrity and accountability, officers will continue to cultivate their own culture in their own way.”* [and] *“It is the lack of internal, systemic controls, and not “a few rotten apples,” that perpetuates problems of misconduct and abuse by police.”* – The Police Foundation Study (see Reference note cclxviii)

[80] “Reminder” suggests that there has been - at least one previous instance, where the Police force was notified of acceptable Police behaviors in such instances

[81] The author is grateful to Attorney Molly Kovel of the NYCLU for the information



DATE: 08/06/2014
TIME: 15:08:40
SER#: 9881632

14

**FINEST MESSAGE**
**General Administrative Information**

TO: ALL COMMANDS

RE: RECORDING OF POLICE ACTION BY THE PUBLIC

MEMBERS OF THE SERVICE ARE REMINDED THAT MEMBERS OF THE PUBLIC ARE LEGALLY ALLOWED TO RECORD (BY VIDEO, AUDIO, OR PHOTOGRAPHY) POLICE INTERACTIONS. THESE INTERACTIONS INCLUDE ARREST AND OTHER SITUATIONS. MEMBERS OF THE SERVICE WILL NOT INTERFERE WITH A PERSON'S USE OF RECORDING DEVICES TO RECORD POLICE INTERACTIONS. INTENTIONAL INTERFERENCE SUCH AS BLOCKING OR OBSTRUCTING CAMERAS OR ORDERING THE PERSON TO CEASE CONSTITUTES CENSORSHIP AND ALSO VIOLATES THE FIRST AMENDMENT.

**Fig. 23** Excerpt of a Memo from NYC Police Chief to Police Depts. on Acceptable Police Behavior in Relation to Public Encounters with Citizen Videographers. Source: NYC Citizen Complaint Review Board Report (2017)

actions had transpired. Importantly, more than a decade full of constitutional violations has taken place. Next, and equally important as the first, involve the points that an illegal, unconstitutional, and plainly rogue Police program was birthed in the City of New York, and by way of “sanctions” from the Mayor of the City of New York, and the Police Commissioner of the New York City, both of whom had separately and individually taken oaths to uphold the law, and the constitution of the land, but then proceeded to violate both. Still, officials have not even been reprimanded, let alone be punished under the law.

From whichever land you the reader may originate, and whichever nation you may be a national of, you will want to discover, how these factors that are being discussed regarding prevailing matters of constitutional interest to those in the U.S., and to her Citizens, affect your own compatriots, and your own rights. In relation to the U.S., one issue is very clear. Americans have historically found it difficult to assert constitutionally assigned privileges, to be able to advocate for those personal privileges granted to natural born citizens under the U.S. constitution. Why have Americans not been cogently assertive of birthrights?[82] Again, an issue not confined to the U.S. Many of our readers can ask the same question of their respective citizens. As discussed earlier within this editorial, civic education, and personal cultivation are essential parts to the securing and continued preservation of one’s rights; our ability to sense any encroachment upon personal rights, or being able to discern the presence, or occurrence of, any outright violation of personal rights.

In the U.S., a significant portion of American population lack command knowledge of national institutions; institutional responsibilities; instruments of law and order; of processes, procedures, attributes and desired manners of governance; relevant national histories or how we are organized as a country, and as ‘common-cause’ people. Furthermore, we lack that knowledge, which is ‘inherently primary’ to citizenship [276], knowledge that would empower, to be able to informedly dispute, or to lawfully be able to advocate validly, on specific issues and/or cases, if necessary. Of these things, Robert Putnam has almost prosaically noted in his book that, “most Americans today feel vaguely and uncomfortably disconnected*”* [277]. Further, Putnam, borrowing from an early twentieth Century writing of Walter Lippman, suggested that perhaps, “we have changed our environment more quickly than we know how to change ourselves.” Reflecting upon Lippman’s remarks there, and in solely appraising the American situation now, this author finds a stern need to deviate from Putnam’s last observation, *for the likes of detachment and the “dumbing-down” that America continues to experience* [278], as Putnam’s own discovery has acknowledged, began long ago. This author notes, as does Putnam, that the quality of American public education over decades had been reaching a crisis [279], which this author submits as the prime cause for our inability to “change ourselves,”” and in turn also the prime cause for our lack of competence and preparedness to match societal needs forward. Putnam noticed that the [U.S.] nationwide decline in social connectedness and civic engagement in such activities as voting, giving, meeting, visiting, newspaper reading, volunteering, and being interested in politics has continued an almost uninterrupted decline for more than 40 years. Such lack of civic engagement and political disconnection result in a general inability to sense, determine and/or act on matters of high consequence, such as the protection of personal and collective rights.

[82] Reference to “Birthrights” here mean the following: 1) those rights that were bequeathed to one at birth, and is therefore guaranteed by the constitution of the country of which one is a national, and 2) those principles that are part of the Universal Declaration of Human Rights (UDHR); if one is a national of a country that is a signatory to the UDHR, the country is responsible to uphold the principles of the UDHR

At present, only a quarter of all Americans (26%) can name the three branches of U.S. Government (down from 38% in 2011), and 33% of Americans cannot name a single branch of Government [280]. 37% of Americans cannot name any of the privileges guaranteed by the First Amendment to the U.S. constitution [281]. When Pew Research asked Americans in 2010, to identify the Chief Justice of the United States Supreme Court [282], more than half (53%) claimed to not know, while another 8% identified former Associate Justice Thurgood Marshall as Chief Justice. It should be mentioned that Justice Marshall had expired in 1993, and had not served the U.S. Supreme Court since 1991, while yet another 4% of Americans identified then U.S. Senate Majority Leader Harry Reid as the Chief Justice. Reid never served in any capacity on the Court, and more importantly, Reid was in service at another branch of government – the Legislative. Yes, to not make the mistake of assigning Reid wrongly, and more fundamentally, as a starter, one would have had to know the difference between serving in the Legislative, vis-à-vis in the Judicial branch of government. Once again, this 'problem,' is not localized to America. More widely, the rise of extremism (any variety) worldwide (as in India, Pakistan, Myanmar, Iraq, China, Germany, Austria, Hungary, Poland, Sweden, Norway etc.) is rooted in a multiplying of inter-generational prejudices, and a decline/erosion in 'human cultivation' at least, one that has fostered an almost willful blindness to the authentic nature of human conditions and compositions. Such blindness, and the character of accompanying subject matter ignorance as detailed herein - leave populations inherently incapable of defending against encroachments upon constitutionally granted privileges, by anyone, including those who believe they are delivering and enforcing 'lawful instructions or orders,' when they could clearly not be.

Success in th*e* fight against injustice is largely dependent upon a heightened level of "knowledge boosted-awareness," of one's living states. An individual could only comprehend fully the severity associated with a sensitive data-breach at a Credit Reporting Bureau, for instance, if one possessed the critical background and the knowledge connected to the working components in the Credit Reporting enterprise and their inter-relationships among other things. In order to mount a capable defense against encroachments upon Personal Privacy or Security, one must understand, and have an appreciation for (without exception) the most basic privileges that are vested to each citizen by constitutions, personal knowledge of limitations or restrictions that can be imposed upon those privileges, and the terms and conditions under which any limitation and or restriction may be imposed. Such personal knowledge is an integral part to understanding the nature of basic citizenship, and being adequately informed on the way to sense, assess, and act on Personal Privacy and Security related encroachments and/or violations.

In the overall, the intention of this Editorial Chapter has been to unearth the many dimensions of the Privacy world, which are seldom surfaced, or discussed. Above all, the focus of the editorial has been to deemphasize the' conventional spotlighting' of Privacy issues that go on, and to highlight the more urgent and fundamental need for a deeper and richer common understanding of Privacy situations, and of the value Privacy poses to the individual, and to society. Another goal of the editorial was to amplify the need to acquire gainful personal knowledge to many important aspects of Privacy and Security, as to be maximally effective, and to be exceedingly valuable within the globally distributed yet, interconnected, interdependent, and interoperable *digitomicy,*[83] as employers, employees, technology enthusiasts, and as Privacy and Security advocates.

Success in our individual and collective attempts to protect and preserve values such as Personal Privacy and Personal Security will depend largely upon each of us, "knowing" and "acting" through lawful and constitutionally privileged means, and by collectively organizing to defend personal freedoms. In motivation to that, we must re-introduce ourselves to the remonstrations of the Late Associate Justice of the Supreme Court of the United States, William J. Brennan, who chided us for being delinquent, and being cavalier in our consignment, or rather, the surrender of 'our very personal powers,' 'the power of self-determination' - over and into - the hands of governments. We must pay heed and homage to Justice Brennan's sharp excoriation of our collective 'stand and streak' – our 'bent and badge' – for not investing the time and effort to learn; to command knowledge vital to our self-determination; to lazily and piningly take up instead: governmental maternalism and paternalism, consigning to *'[g]overnments more power over our lives than ever before,'* and of it, *'we seem not more concerned, but more indifferent to the consequences of …surrender.'* [283]

**Funding** No Funding was received toward the composition of this editorial chapter.

**Compliance with ethical standards**

**Conflict of interest** No conflict of interest exists.

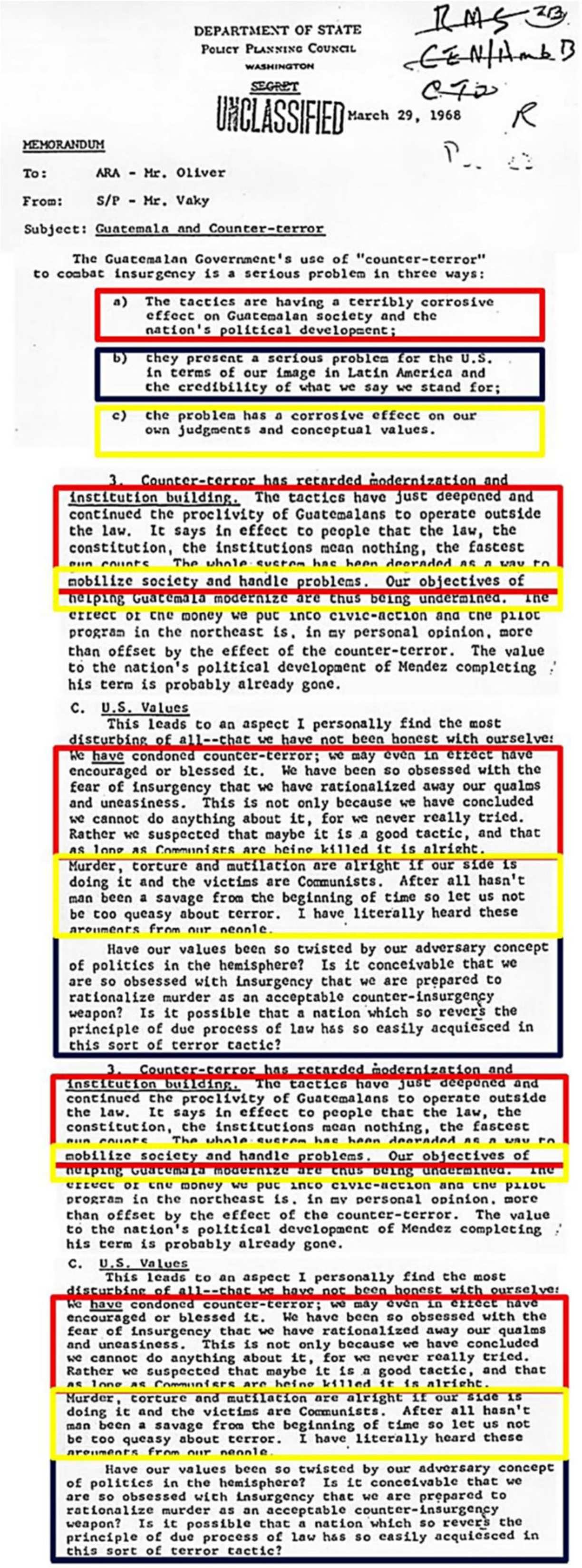
**Ethical approval** No experimentation involving human or animal was conceived or executed in relation to the writing of this editorial manuscript.

**Informed consent** Not Applicable.

[*] The author presents his regrets to the readership in relation to the decision to include a picture (Fig. 18), which could be intellectually, spiritually, and/or emotionally disturbing for the reader. The picture keenly emphasizes for the reader, the product of 'citizen-on-citizen' evil and criminality occurring in present day India.

[83] See footnote 60

## Appendix



DEPARTMENT OF STATE
POLICY PLANNING COUNCIL
WASHINGTON

~~SECRET~~
UNCLASSIFIED March 29, 1968

RMS 23
CEN/Amb B
C72
R
P

MEMORANDUM

To: ARA - Mr. Oliver

From: S/P - Mr. Vaky

Subject: Guatemala and Counter-terror

The Guatemalan Government's use of "counter-terror" to combat insurgency is a serious problem in three ways:

a) The tactics are having a terribly corrosive effect on Guatemalan society and the nation's political development;

b) they present a serious problem for the U.S. in terms of our image in Latin America and the credibility of what we say we stand for;

c) the problem has a corrosive effect on our own judgments and conceptual values.

3. Counter-terror has retarded modernization and institution building. The tactics have just deepened and continued the proclivity of Guatemalans to operate outside the law. It says in effect to people that the law, the constitution, the institutions mean nothing, the fastest gun counts. The whole system has been degraded as a way to mobilize society and handle problems. Our objectives of helping Guatemala modernize are thus being undermined. The effect of the money we put into civic-action and the pilot program in the northeast is, in my personal opinion, more than offset by the effect of the counter-terror. The value to the nation's political development of Mendez completing his term is probably already gone.

C. U.S. Values

This leads to an aspect I personally find the most disturbing of all--that we have not been honest with ourselves We have condoned counter-terror; we may even in effect have encouraged or blessed it. We have been so obsessed with the fear of insurgency that we have rationalized away our qualms and uneasiness. This is not only because we have concluded we cannot do anything about it, for we never really tried. Rather we suspected that maybe it is a good tactic, and that as long as Communists are being killed it is alright. Murder, torture and mutilation are alright if our side is doing it and the victims are Communists. After all hasn't man been a savage from the beginning of time so let us not be too queasy about terror. I have literally heard these arguments from our people.

Have our values been so twisted by our adversary concept of politics in the hemisphere? Is it conceivable that we are so obsessed with insurgency that we are prepared to rationalize murder as an acceptable counter-insurgency weapon? Is it possible that a nation which so revers the principle of due process of law has so easily acquiesced in this sort of terror tactic?

3. Counter-terror has retarded modernization and institution building. The tactics have just deepened and continued the proclivity of Guatemalans to operate outside the law. It says in effect to people that the law, the constitution, the institutions mean nothing, the fastest gun counts. The whole system has been degraded as a way to mobilize society and handle problems. Our objectives of helping Guatemala modernize are thus being undermined. The effect of the money we put into civic-action and the pilot program in the northeast is, in my personal opinion, more than offset by the effect of the counter-terror. The value to the nation's political development of Mendez completing his term is probably already gone.

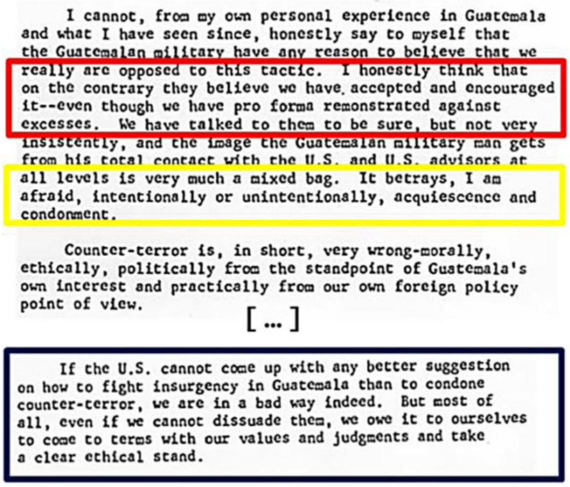
C. U.S. Values

This leads to an aspect I personally find the most disturbing of all--that we have not been honest with ourselves We have condoned counter-terror; we may even in effect have encouraged or blessed it. We have been so obsessed with the fear of insurgency that we have rationalized away our qualms and uneasiness. This is not only because we have concluded we cannot do anything about it, for we never really tried. Rather we suspected that maybe it is a good tactic, and that as long as Communists are being killed it is alright. Murder, torture and mutilation are alright if our side is doing it and the victims are Communists. After all hasn't man been a savage from the beginning of time so let us not be too queasy about terror. I have literally heard these arguments from our people.

Have our values been so twisted by our adversary concept of politics in the hemisphere? Is it conceivable that we are so obsessed with insurgency that we are prepared to rationalize murder as an acceptable counter-insurgency weapon? Is it possible that a nation which so revers the principle of due process of law has so easily acquiesced in this sort of terror tactic?

## APPENDIX (A)

*Vaky – Oliver Declassified Memo on "Guatemala & Counter-Terror" & "The Ethical Policy Imperative"*
**Source:** National Security Archive,
GWU, Washington, D.C.



I cannot, from my own personal experience in Guatemala and what I have seen since, honestly say to myself that the Guatemalan military have any reason to believe that we really are opposed to this tactic. I honestly think that on the contrary they believe we have accepted and encouraged it--even though we have pro forma remonstrated against excesses. We have talked to them to be sure, but not very insistently, and the image the Guatemalan military man gets from his total contact with the U.S. and U.S. advisors at all levels is very much a mixed bag. It betrays, I am afraid, intentionally or unintentionally, acquiescence and condonment.

Counter-terror is, in short, very wrong-morally, ethically, politically from the standpoint of Guatemala's own interest and practically from our own foreign policy point of view.

[...]

If the U.S. cannot come up with any better suggestion on how to fight insurgency in Guatemala than to condone counter-terror, we are in a bad way indeed. But most of all, even if we cannot dissuade them, we owe it to ourselves to come to terms with our values and judgments and take a clear ethical stand.

## References

1. Bell D.. The coming of post-industrial society; a venture in social forecasting. Basic Books, New York, 1973.
2. Brittan L. Global Partners: Japan and the European Union (Speech - Vice-President of the European Commission), National Press Club - EU-Japan Cooperation Week, Tokyo, Japan, 29 September 1997 http://europa.eu/rapid/press-release_SPEECH-97-196_en.htm
3. Examples of Environmental Disasters Caused By Man. Bhopal, India: Taylor, Alan; "Bhopal: The World's Worst Industrial Disaster, 30 Years Later," The Atlantic, 2 December 2014 https://www.theatlantic.com/photo/2014/12/bhopal-the-worlds-worst-industrial-disaster-30-years-later/100864/ Chernobyl, Ukraine: Lallanilla, Marc; "Chernobyl: Facts About the Nuclear Disaster" (26 April, 1986), LiveScience, 25 September 2013 https://www.livescience.com/39961-chernobyl.html Fukushima, Japan: Wolchover, Natalie; "Timeline of Events at Japan's Fukushima Nuclear Reactors" (11 March 2011), LiveScience, 17 March 2011 https://www.livescience.com/13294-timeline-events-japan-fukushima-nuclear-reactors.html London's Killer Fog of 1952: Deamer, Kacey; "Mystery Solved! Cause of London's 1952 'Killer Fog' Revealed" (5–9 December 1952), LiveScience, 9 December 2016 https://www.livescience.com/57157-mystery-of-london-killer-fog-solved.html Seveso, Italy: De Marchi, B et. al; "Seveso: A paradoxical classic disaster" (10 July 1976), United Nations University ("Community Responses to Industrial Hazards," Environment Programme), November 1992 [Town of Seveso became known as "Italy's Hiroshima" after the Dioxin crisis] http://archive.unu.edu/unupress/unupbooks/uu21le/uu21le09.htm#4%20seveso:%20a%20paradoxical%20classic%20disaster Aral Sea, Central Asia: Lindsey, Rebecca; "Shrinking Aral Sea," NASA Earth Observatory, 25 August 2000, https://earthobservatory.nasa.gov/Features/WorldOfChange/aral_sea.php Love Canal, New York: Kleiman, Jordan; "Love Canal: A Brief History," SUNY - Geneseo, 2017 https://www.geneseo.edu/history/love_canal_history
4. Dilliard I. Mr. Justice Brandeis, Great American; Press Opinion and Public Appraisal, The Modern View Press, St. Louis, MO (USA), 1941 [In: "Life Argues Against Anti-Semitism", The Christian Century, October 15, 1941].
5. Dilliard I. Mr. Justice Brandeis, Great American; Press Opinion and Public Appraisal," The Modern View Press, St. Louis, MO (USA), 1941 [In: "A Robust and Consistent Faith", The Nation, October 11, 1941].
6. Schwab K.. The Fourth Industrial Revolution: what it means, how to respond, World Economic Forum (WEF)/Global Agenda, Geneva, Switzerland, 14 January 2016 https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/
7. Justice K. S. Puttaswamy (Retd.) and ANR. (Petitioners) versus Union of India and ORS et. al. (Respondents), Writ Petition (Civil) No: 494 of 2012, In The Supreme Court of India, New Delhi, India, 24 August, 2017 http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf
8. Lever A. Privacy: Restrictions and Decisions, APA Newsletter on Philosophy and Law, Vol. 13, No: 1, Fall 2013 https://c.ymcdn.com/sites/www.apaonline.org/resource/resmgr/law_newsletter/lawv13n1.pdf
9. Westin AF. Privacy & Freedom, Atheneum, New York, 1967.
10. Post Robert C. Three concepts of privacy, faculty scholarship series – paper 185, Yale Law School, New Haven, 2001.
11. Lever, *Supra,* note 8.
12. Warren SD, Brandeis LD. The Right to Privacy, Harvard Law Review, Vol. IV, No. 5, 15 December 1890.
13. Richardson J. Law and the Philosophy of Privacy, Routledge/GlassHouse, Oxford, England, 2016.
14. The Right to Privacy in Nineteenth Century America, Harvard Law Review, Vol. 94, No. 8 June 1981 [Provided here as an example to the seemingly endless sea of references to the 1890 Warren-Brandeis article in Harvard Law Review].
15. Warren and Brandeis, *Supra* note 12.
16. Edwin Lawrence (E.L.) Godkin; "The Rights of the Citizen: IV. To His Own Reputation," Scribners, July 1890.
17. Godkin EL. Libel and its Legal Remedy," Journal of Social Science Containing The Transactions of The American Association (No: XII) (F. B. Sanborn, Ed.), Saratoga Papers of 1880 - Part I, A. Williams & Co., Boston, MA, USA, 1880 AND E.L. Godkin; "Libel and its Legal Remedy," The Atlantic Monthly, Vol. 46, No: 278, December 1880.
18. Cooley TMcI. A Treatise On The Law Of Torts: Or The Wrongs Which Arise Independently Of Contract [Cooley On Torts, 2nd Ed.], Callahan & Co., Chicago, IL, 1888.
19. *Ibid*.
20. Wilson K, Salas E, Priest H, Andrews D. Errors in the heat of battle: Taking a closer look at shared cognition breakdowns through teamwork, U.S. Air Force Research Laboratory Report (AFRL-RH-AZ-JA-2007-0003, Released as an article, Journal of Human Factors, Vol. 49, No. 2, April 2007), U.S. Air Force Research Laboratory/RHA, Warfighter Readiness Research Division, Mesa, AZ., April 2007.
21. Barks PB. Anything But: Joint Air-Ground Training at the U.S. Army Ground Combat Training Centers" [Joint Forces Staff College (JFSC) Report JFSC 25789], Joint Advanced Warfighting School, Joint Forces Staff College, Norfolk, VA., 3 April 2009.
22. From Desert Storm to 2025: Close Air Support in the 21st Century, Air Command and Staff College (1998), cited in: Barks, Phillip; "Anything But: Joint Air-Ground Training at the U.S. Army Ground Combat Training Centers" (Note xxi).
23. Wilson K, Salas E, Priest H, Andrews D. *Supra*, Note 20.
24. Shappell SA, Wiegmann DA. The Human Factors Analysis and Classification System–HFACS [FAA Report# DOT/FAA/AM-00/7], U.S. Federal Aviation Administration (FAA)/Office of Aviation Medicine, Washington, D.C., February 2000.
25. Raimon RL, Stoikov V. The Quality of the Labor Force, ILR Review, Vol. 20, No. 3, 1 April 1967 AND SAMPLE HR Reading: Gimpelson, V; "Does the Russian Economy Need Human Capital? Ten Doubts," Russian Education & Society, Vol. 58 Issue 11, 2016.
26. Percin A. Le Massacre De Notre Infanterie 1914–1918, Albin Michel, Paris, 1921.
27. Krakauer Explores Pat Tillman's Death And Cover-Up NPR - All Things Considered (U.S.), 14 September 2009 https://www.npr.org/templates/story/story.php?storyId=112816210 AND Soldier: Army ordered me not to tell truth about Tillman, CNN, 25 April 2007 http://www.cnn.com/2007/POLITICS/04/24/tillman.hearing/ AND Hart, Hugh; "Documentary examines Tillman's death, cover-up," SFGATE (San Francisco Chronicle - HEARST), 15 August 2010 http://www.sfgate.com/movies/industrybuzz/article/Documentary-examines-Tillman-s-death-cover-up-3255785.php.
28. Manning RJ. Datums and Grids – What You Don't Know Can Kill You, Journal of Military Intelligence, October–December 2002Manning, Richard J; "Datums and Grids – What You Don't Know Can Kill You", Journal of Military Intelligence, October–December 2002.
29. *Ibid*.

30. Provided As An Example Only: "Aadhaar challenged in SC: 9-judge bench to decide whether you have the right to privacy" Press Trust of India 19 July 2017 http://www.firstpost.com/india/constitutional-validity-of-aadhaar-sc-sets-up-9-judge-constitution-bench-to-hear-pleas-3826521.html AND "Every aspect of right to privacy is not fundamental, Centre tells Supreme Court", Press Trust of India, 27 July 2017 http://www.firstpost.com/india/every-aspect-of-right-to-privacy-is-not-fundamental-centre-tells-supreme-court-3861901.html (provided as examples only).
31. Provided As An Example Only: Soutik Biswas; "Aadhaar: Are a billion identities at risk on India's biometric database", BBC India, 4 May 2017 http://www.bbc.com/news/world-asia-india-39769322 AND Amit Anand Choudhary; "Citizens don't have absolute right over their bodies: Government", Times of India, May 3, 2017 http://timesofindia.indiatimes.com/india/citizens-dont-have-absolute-right-over-their-bodies-government/articleshow/58486260.cms AND "Citizens don't have 'absolute' right over their bodies, privacy complaint is 'bogus' - Indian govt", Russia Today (RT) 3 May, 2017 https://www.rt.com/news/386953-india-government-bodies-privacy/.
32. Mathews R. On protecting & preserving personal privacy in interoperable global healthcare venues [Collection on Social Implications of Technologies], Journal of Health & Technology, Volume 6, Issue 1, 2016 https://link.springer.com/article/10.1007/s12553-016-0126-6.
33. Schwab, *Supra,* Note 6.
34. Citing the author in: "Unreliability of Community Memories and Its Relativity To Blockading of U.S. Scientific Progress" [Samuel Keene], IEEE Transactions on Reliability [Reliability Society], Vol 58, No. 2, 2009 http://ieeexplore.ieee.org/stamp/stamp.jsp?reload=true&tp=&arnumber=5062554 or http://rs.ieee.org/annual-technology-reports/39-2008.html.
35. Westin, *Supra,* Note 9.
36. Thomson JJ. Rights, Restitution & Risk - Essays in Moral Theory [William Parent, Ed.], Harvard University Press, Cambridge, 1986.
37. Miller AR. The Assault on Privacy Computers, Data Banks, and Dossiers, The University of Michigan Press, Ann Arbor, MI (USA), 1971.
38. Gellman R, Dixon P. Online Privacy: A Reference Handbook, ABC-CLIO, Santa Barbara, 2011.
39. Brotton J. A History of The World In Twelve Maps, Allen Lane, London, UK, 2012.
40. Holland T. A History of The World in Twelve Maps by Jerry Brotton – review; The Guardian, 24 August 2012. https://www.theguardian.com/books/2012/aug/24/history-world-twelve-maps-review *(emphasis not in the original).*
41. O'Flynn SL. Place and Identity in Auto-topographic Metanarrative [Ph.D. Dissertation], Dept. of English, University of Toronto, Canada, 2004.
42. Branch J. Mapping the Sovereign State: Technology, Authority, and Systemic Change", International Organization Vol. 65, Winter 2011.
43. *Ibid*.
44. O'Flynn SL. Place and Identity in Auto-topographic Metanarrative, *Supra* Note 41.
45. Dee J, Preface, In "The Elements of Geometrie of The Most Ancient Philosopher Euclid of Megara" [Faithfully (now first) translated into the English tongue, by H. Billingsley, Citizen of London. Whereunto are annexed certain Scholies, Annotations, and Inventions of the best Mathematicians, both of the time past, and this our age.], John Day, London, 1570. ** Jerry Brotton notes this in another one of his works, "Trading Territories: Mapping the early modern world," Reaktion Books, London, UK, 1997.
46. "How Google represents disputed borders between countries: In 12 regions, it presents different borders to different audiences depending on where they are," The Economist/The Economist explains, 4 September, 2014. https://www.economist.com/blogs/economist-explains/2014/09/economist-explains-1.
47. *Ibid*.
48. Two Examples of Diverging Privacy Related Cases Launched by a SINGLE Party: 1) "Maximillian Schrems v Data Protection Commissioner" (Case C-362/14), Court of Justice of the European Union, 6 October 2015 AND "The Data Protection Commissioner (IE) v. Facebook Ireland Ltd., and Maximillian Schrems," Judgement To Refer - The High Court (Commercial) [2016 No. 4809 P.], 3 October 2017 https://www.dataprotection.ie/docs/EN/03-10-2017-Irish-High-Court-grants-the-Data-Protection-Commissioner-its-CJEU-referral-in-DPC-v-Facebook-Ireland-and-Maximilian-Schrems/m/1666.htm [This author expects that upon consideration, the CJEU will rule against the use of Standard Contractual Clauses (SCCs) as a means to facilitate the transfer of sensitive PII between the EU and the US. Such a ruling will likely be more impacting for a country such as India].
49. Seltzer W, Anderson M. Using Government Statistical Systems to Target Businesses and Vulnerable Population Groups: Examples and Issues In: "Statistical Methods for Human Rights" [J. Asher et al., Eds.], Springer 2008.
50. Kirk J. Estonia Invalidates Digital Certificates Over Crypto Crack Unpatched Infineon Chip Peril as Researchers Speed Up Encryption Key Attack, Bank Info Security, 8 November 2017 https://www.bankinfosecurity.com/estonia-invalidates-digital-certificates-over-crypto-crack-a-10440.
51. Vahtla A. Cracking of one ID card would require Estonia to deactivate 750,000 cards (3) Eesti Rahvusringhääling (Estonian Public Broadcaster) err.ee, 4 October 2017 http://news.err.ee/634222/cracking-of-one-id-card-would-require-estonia-to-deactivate-750-000-cards.
52. *Ibid*.
53. Vahtla A. Estonia to provide €670,000 in support for Mobile-ID access development, Eesti Rahvusringhääling (Estonian Public Broadcaster) err.ee, 5 October 2017 http://news.err.ee/634560/estonia-to-provide-670-000-in-support-for-mobile-id-access-development.
54. Kirk, Jeremy *Supra*, Note 50.
55. Sample reading only: Sterling, Toby; "Europol: Ransomware top threat in 2017 cybercrime 'epidemic'," Reuters, 27 September 2017 https://www.reuters.com/article/legal-cyber-europol/europol-ransomware-top-threat-in-2017-cybercrime-epidemic-idUSKCN1C22C8 AND Schwartz, Mathew J; "Financial Sector Under Increasing Cybercrime Threat – Europol Chief Sounds Warnings Over Ransomware," Bank Info Security, 9 November 2017 https://www.bankinfosecurity.com/financial-sector-under-increasing-cybercrime-threat-a-10444 AND Kovacs, Eduard; "Symantec Tricked Into Revoking Certificates Using Fake Keys," SecurityWeek, 21 July 2017 http://www.securityweek.com/symantec-tricked-revoking-certificates-using-fake-keys.
56. Adams M. Why the OPM Hack Is Far Worse Than You Imagine, Lawfare (Cybersecurity), 11 March 2016 https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine.
57. Hatmaker T. Senators push to ditch Social Security numbers in light of Equifax hack, TechCrunch (TC), 8 November 2017 https://techcrunch.com/2017/11/08/are-social-security-numbers-going-away/.
58. Ranieri L, Shay S. Let's not waste the Equifax crisis (Opinion), The Hill, 8 November 2017 http://thehill.com/opinion/cybersecurity/359390-lets-not-waste-the-equifax-crisis
59. Cameron D. Report: Equifax Warned of Vulnerability Six Months Before Attack, Took No Action, Gizmodo, 26 October 2017

https://gizmodo.com/report-equifax-warned-of-vulnerability-six-months-befo-1819880735.

60. Cameron D. Equifax and Yahoo Complain They Are Helpless Against State-Sponsored Hacks, Gizmodo, https://gizmodo.com/equifax-and-yahoo-complain-they-are-helpless-against-st-1820256817.
61. Chabrow E. Former Yahoo CEO: Stronger Defense Couldn't Stop Breaches – Marissa Mayer Testifies on the Challenges of Halting State-Backed Persistent Attacks," Bank Info Security, 8 November 2017 https://www.bankinfosecurity.com/mayer-strengthened-defense-couldnt-stop-massive-breaches-a-10442.
62. Goodin D. Equifax website borked again, this time to redirect to fake Flash update Malware researcher encounters bogus download links during multiple visits, arsTECHNICA, 12 October 2017 https://arstechnica.com/information-technology/2017/10/equifax-website-hacked-again-this-time-to-redirect-to-fake-flash-update/.
63. Proclamation 1898, "CENSUS INQUIRIES," President Herbert Hoover, November 22, 1929, In: "Herbert Hoover: Proclamations and Executive Orders, March 4, 1929 to March 4, 1933." Public Papers of the Presidents of the United States [Book 1]. University of Michigan, Ann Arbor. https://quod.lib.umich.edu/p/ppotpus/4731703.proc.001/57?rgn=full+text;view=image.
64. Anderson, Margo and Seltzer, William; "Challenges to the Confidentiality of U.S. Federal Statistics, 1910–1965," Journal of Official Statistics, Vol. 23, No. 1, 2007.
65. *Ibid*.
66. Seltzer W, Anderson M. The Dark Side of Numbers: The role of Population Data Systems in Human Rights Abuses, Social Research, Vol. 68, No. 2, Summer 2001 AND Seltzer W; "The Dark Side of Numbers: Updated." In: "Bevölkerungsforschung und Politik in Deutschland im 20. Jahrhundert" [Population Research and Politics in Germany in the 20th Century, [Mackensen, Rainer (Eds.)]], VS Verlag für Sozialwissenschaften, [Publisher for Social Sciences], 2006.
67. Seltzer W, Anderson M. After Pearl Harbor: The Proper Role of Population Data Systems in Time of War, Session on "Human Rights, Population Statistics, and Demography: Threats and Opportunities," Population Association of America, Annual Meeting, March 23–25, 2000, Los Angeles, CA. https://ww2.amstat.org/about/statisticiansinhistory/blocks/dsp_paperinfo.cfm?PaperID=1&pf=yes.
68. *Ibid*.
69. Seltzer W, Anderson M. Census Confidentiality under the Second War Powers Act (1942–1947), Presented in: Session 97: Confidentiality, Privacy, and Ethical Issues in Demographic Data, at Population Association of America - Annual Meeting, March 29–31, New York, NY, 2007.
70. Watanabe T. In 1943, Census released Japanese Americans' data," The Los Angeles Times, 31 March 2007 http://articles.latimes.com/2007/mar/31/nation/na-census31.
71. El-Nasser H. Papers show Census role in WWII camps," USA TODAY, 30 March 2007 http://usatoday30.usatoday.com/news/nation/2007-03-30-census-role_N.htm.
72. Minkel JR. Confirmed: The U.S. Census Bureau Gave Up Names of Japanese-Americans in WW II – Government documents show that the agency handed over names and addresses to the Secret Service, Scientific American, 30 March 2007. https://www.scientificamerican.com/article/confirmed-the-us-census-b/.
73. Black E. IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation," Dialog Press, Washington, D.C., 2009.
74. *Ibid*.
75. *Ibid*.
76. *Ibid*.
77. "An IBM punch card could only be used once. After a period of months, the gargantuan stacks of processed cards were routinely destroyed. Billions more were needed each year by the Greater Reich and its Axis allies, requiring a sophisticated logistical network of IBM authorized pulp mills, paper suppliers, and stock transport. Sales revenue for the lucrative supply of cards was continuously funneled to IBM via various modalities, including its Geneva nexus." AND "The Third Reich consumed cards at an almost fantastic rate. Projected use by 1943 was 1.5 billion [a year] just within the Reich. Holleriths could not function without cards. Watson controlled the cards." – Black, 2009.
78. *Ibid*.
79. Klick M. Guatemala Calling: Lynchings and the Politics of Inequality," Political Violence At A Glance (Denver Dialogues), 4 August 2015 https://politicalviolenceataglance.org/2015/08/04/guatemala-calling-lynchings-and-the-politics-of-inequality/ AND Staff writer; "16-year-old girl in Guatemala beaten, burned alive by mob," Al Arabiya News, 23 May 2015 https://english.alarabiya.net/en/News/world/2015/05/23/16-year-old-girl-in-Guatemala-beaten-burned-alive-by-mob-.html.
80. Bahbah B, Butler L. Israel and Latin America: The Military Connection, Macmillan/Palgrave Macmillan, London, UK, 1986.
81. Ibid [emphasis not in the original].
82. Statement in a public lecture by Yohanah Ramati, former editor of the Israeli journal The Economist and member of the Foreign Relations Committee during the Likud government (1977–1984), Florida International University, Bay Vista campus, March 6, 1985 CITED IN: Rubenberg, Cheryl; "Israel and Guatemala Arms, Advice and Counterinsurgency," Middle East Research & Information Project [MER 281] - "Activism," Winter 2016 http://www.merip.org/mer/mer140/israel-guatemala#_1_.
83. Bahbah and Butler, *Supra*, Note 80.
84. Haaretz Editorial. Israel Is Arming Criminals – Lawmakers from across the spectrum should come together to put an immediate stop to Israel's weapons sales to Myanmar, where crimes against humanity are being committed, Haaretz (Tel Aviv, Israel), 27 September 2017 https://www.haaretz.com/opinion/editorial/1.814469
85. Nairn A, Simon J-M. Bureaucracy of Death: Guatemala's civilian government faces the enemy within, The New Republic, 30 June 1986 [And Supplemental Reading] Hood, Lucy; "CHRONICLE OF ANGUISH." "Jean-Marie Simon spent seven years photographing Central America's largest country. Her book, 'Guatemala: Eternal Spring - Eternal Tyranny', documents life in a land of contrasts," The Christian Science Monitor, 16 March 1988 https://www.csmonitor.com/1988/0316/zsimon.html.
86. Schirmer J. The Guatemalan Military Project: A Violence Called Democracy," University of Pennsylvania Press, Philadelphia, PA, 1998 [and Supplementally] Thomas, Baylis; "The Dark Side of Zionism: Israel's Quest for Security through Dominance" [History of Israel's Global Weapons Sales], Lexington Books, Lanham, MD., USA, 2009.
87. Hunter J. Israeli Foreign Policy: South Africa & Central America, " South End Press, Boston, MA, USA, 1987.
88. "Guatemala, Memory of Silence: Tzínil Na'tab'al," Report of the Commission for Historical Clarification (Comisión para el Esclarecimiento Histórico) [Conclusions and Recommendations] The United Nations, 1999.
89. *Ibid*.
90. *Ibid*.
91. Haaretz Editorial. Human Rights in Israel Are in Jeopardy – Israel ratified the Universal Declaration of Human Rights, but it is hard to say the Knesset members are bound to it or to its spirit and principles," Haaretz (Tel Aviv, Israel), 6 December 2011 https://www.haaretz.com/human-rights-in-israel-are-in-jeopardy-1.399755.
92. Haaretz - "Israel Is Arming Criminals," *Supra*, note 84.

93. See Conclusion, for a brief discussion of Law Enforcement personnel, their actions and relationship to Privacy and Security.

94. 'Between 2001 and 2015, Rwanda's real GDP growth averaged at about 8% per annum.' Rwanda - Country Overview, The World Bank http://www.worldbank.org/en/country/rwanda/overview.

95. "Rwanda: From hatred to reconciliation - The story of the 1994 Rwandan genocide told through the prism of the media, exploring their role then and today", Al Jazeera, Al Jazeera World, 29 September 2015 http://www.aljazeera.com/programmes/aljazeeraworld/2015/09/rwanda-hatred-reconciliation-150929140405404.html

96. Pilling D, Barber L. Interview: Kagame insists 'Rwandans understand the greater goal'" The Financial Times (FT), 27 August 27 2017 https://www.ft.com/content/a2838936-88c6-11e7-bf50-e1c239b45787.

97. Reports of findings by Amnesty International on Human Rights related activities in Rwanda (2016–2017), Amnesty International International Secretariat, London, UK https://www.amnesty.org/en/countries/africa/rwanda/ AND An Assessment of Human Rights Related Societal Progress in Rwanda - 2016, Human Rights Watch, New York City, NY., USA https://www.hrw.org/world-report/2017/country-chapters/rwanda.

98. "National ICT Strategy and Plan," Ministry of Youth and ICT/Office of the President, Kigali, Rwanda, 2015 http://www.rdb.rw/uploads/tx_sbdownloader/NICI_III.pdf AND "National Data Revolution Plan," Ministry of Youth and ICT, Republic of Rwanda, Kigali, Rwanda, April 2017 http://www.statistics.gov.rw/publication/rwanda-national-data-revolution-and-big-data.

99. Sample reading: Verdeja, Ernesto; "The Political Science of Genocide: Outlines of an Emerging Research Agenda," Perspectives on Politics, Vol.10, No: 2, 2012 AND Kohen, Ari; Zanchelli, Michael ; Drake, Levi; "Personal and Political Reconciliation in Post-Genocide Rwanda," Social Justice Research," Vol.24, No: 1, 2011 AND Totten, Samuel; "The State and Future of Genocide Studies and Prevention: An Overview and Analysis of Some Key Issues," Genocide Studies and Prevention, Vol. 6, No: 3, December 2011.

100. *Ibid*.

101. Nsengimana JP. Reflections upon periclitations in privacy: perspectives from Rwanda's digital transformation," The Journal of Health and Technology, 12 July 2017 https://doi.org/10.1007/s12553-017-0196-0.

102. Keane, John; "Global Civil Society?," Cambridge University Press, New York, NY., 2003.

103. Justice K. S. Puttaswamy (Retd.), *Supra*, Note 7.

104. Satpathy T. The Aadhaar: " Evil " Embodied as Law," The Journal of Health and Technology, Springer, June 2017 https://link.springer.com/article/10.1007/s12553-017-0203-5.

105. Voltaire, M. de [François-Marie Arouet]; "The Philosophy of History," Robert Urie, Glasgow, Scotland, 1766.

106. "If the Buddha's death date is brought down first from 544 to 480 B.C., finally all the way to 371, then "[t]he Buddha becomes younger than Pericles (c. 492–420 B.C.), Socrates (461—599 B.C.) and Pythagoras. Vais'ali, the ancient republic, becomes younger than Athens…"" – In: McEvilley, Thomas; "The Shape of Ancient Thought: Comparative Studies in Greek and Indian Philosophies," Allworth Press, New York, NY, 2002 AND Chakrabarti, Dilip K; "Colonial Indology: Sociopolitics of the Ancient Indian Past," Munshiram Manoharial Publishers, New Dehli, India, 1997.

107. Sinha BP. Ancient Cities of Bihar in Archaeology and Literature, Man and Environment (Journal of the Indian Society for Prehistoric and Quaternary Studies), Vol-XX, Number 1, January–June 1995.

108. A State where the functioning government had within, representatives whom the people of the State had chosen to represent them in government processes in all matters of governance. The people also enjoyed common rights and privileges.

109. "Kautilya's Arthashastra" [Translated into English by R. Shamasastry], Government Press, Bangalore [Bangaluru], India, 1915.

110. *Ibid*.

111. *Ibid*.

112. *Ibid*.

113. Sidney, Algernon; "Discourses Concerning Government" [Vol. I], G. Hamilton & J. Balfour, Edinburgh, Scotland, 1750 (Was written in 1698 as a defense against propositions presented in "Patriarcha") [Emphasis not in the original].

114. *Ibid*.

115. Ochlocracy is: "A government where the authority is in the hands of the multi-tude; the abuse of a democracy." - Vaumene Dict. du Language Politique. Noted In: Shumaker, By Walter A and Foster Longsdorf, George; "The Cyclopedic Law Dictionary: Comprising the Terms and Phrases of American Jurisprudence, Including Ancient and Modern Common Law, International Law, and Numerous Select Titles From The Civil Law, The French and The Spanish Law Etc, Etc." [James Christopher Cahill - 2nd Edition], Callaghan & Company, Chicago, IL, 1922.

116. Letter from John Adams to John Taylor (No. 18), 17 December 1814, United States National Archives, Washington, D.C., https://founders.archives.gov/documents/Adams/99-02-02-6371.

117. Marshall J. The Life of George Washington, Commander in Chief of the American Forces, During the War which Established the Independence of His Country, and First President of the United States (Vol. V, Chap IX), C.P. Wayne, Philadelphia, PA, 1807 [Generally referred to, also as: "Marshall's Washington"].

118. "I am constrained to ask, Is this a way to run a constitutional government? Is this a way to lead a Republic? I hear so many of our Senators talk about this "democracy." This is not a democracy." The Late US Senator Robert C. Byrd (D-W.VA) "Connecting The Dots on Iraq," Congressional Record - US Senate, 28 June 2002.

119. Follett MP. Democracy Not the Crowd: Our Popular Delusion (Chapter XVIII) In: "The New State: Group Organization The Solution of Popular Government" [3rd Edition], Longmans, Green & Co., New York, NY, 1920.

120. *Ibid*.

121. As an example, Cornelius Castoriadis emphasized the corruptive influences of something "ridiculously called contemporary "individualism,"" which he noted as having corrupted people's most basic understanding of 'autonomy,' in relation to "Democracy." Castoriadis thought that "autonomy (the effective freedom) of all is, and has to be, a fundamental concern of each [in society]. (The tendency to "forget" this self-evident fact is one of the innumerable ways in which contemporary "individualism" tries to stack the deck.)" – Castoriadis, Cornelius; "Democracy as Procedure and Democracy as Regime," Constellations, Volume 4, Number 1, 1997 [Author's comments: such inability to differentiate as Castoriadis described, among other things, amount to being fundamental to that inability of populations in developed nations to put forward a united front in such areas a Privacy Protections, and Personal Security. Sweep of "contemporary individualism" related notions has aided the erasure of a deeper and richer understanding of the value of "effective freedom."]

122. "The Universal Declaration of Human Rights is the Most Universal Document in the World," United Nations – Office of the High Commissioner (Human Rights), Geneva, Switzerland, August 2017 http://www.ohchr.org/EN/UDHR/Pages/WorldRecord.aspx.

123. "Finance and Opportunity in India" (Address by Raghuram Rajan - Reserve Bank of India chairman), The Twentieth Lalit Doshi

Memorial Lecture, Mumbai, India, 11 August 2014 https://www.rbi.org.in/scripts/BS_SpeechesView.aspx?Id=908.

124. Allen F, Chakrabarti R, De S, Qian J, Qian M. Financing firms in India (Report No: WPS 3975), World Bank, Washington, DC, USA, 2006 http://documents.worldbank.org/curated/en/152071468269084445/Financing-firms-in-India [emphasis not in the original].

125. Vaishnav M. When Crime Pays: Money and Muscle in Indian Politics," Yale University Press, New Haven, CT., USA., 2017.

126. *Ibid*.

127. Ochlocracy, *Supra*, Note 115.

128. Oberst, By Robert C; Malik, Yogendra K; Kennedy, Charles; Kapur, Ashok; Lawoti, Mahendra; Rahman, Syedur and Ahmad, Ahrar; "Government and Politics in South Asia" [7th Edition], Westview Press/Perseus Book Group, Boulder, CO., USA, 2014 [emphasis not in the original].

129. "Modi promises tough steps to end corruption," IndiaToday.in, 19 August 2014 http://indiatoday.intoday.in/story/narendra-modi-rally-kaithal-haryana/1/377817.html.

130. Thomas M. Despite Modi's anti-corruption drive, 70% of Indians must still pay bribes for basic services," Quartz India, March 07, 2017. https://qz.com/926239/despite-modis-anti-corruption-drive-70-indians-must-still-pay-bribes-for-basic-services/.

131. A Statement by David C. Mulford, U.S. Ambassador to India – "Issue of Gujarat Chief Minister Narendra Modi's Visa Status," Roosevelt House [U.S. Embassy], New Delhi, India, 21 March 2005 AND (Supplemental) Mann, James; "Why Narendra Modi Was Banned From the U.S.: Narendra Modi is the only person ever denied a U.S. visa based on a little-known law on religious freedom," The Wall Street Journal, 2 May, 2014 https://www.wsj.com/articles/why-narendra-modi-was-banned-from-the-u-s-1399062010.

132. HRD Min Smriti Irani wants ancient texts included in school syllabi, FIRSTPOST (FP Staff), 01 June 2014 http://www.firstpost.com/politics/hrd-min-smriti-irani-wants-ancient-texts-included-in-school-syllabi-1551693.html AND Kumar, Raksha; "Hindu right rewriting Indian textbooks Books by Hindu nationalists merging myth with reality proliferate in PM Modi's home state of Gujarat," Al Jazeera, 4 November 2014 http://www.aljazeera.com/indepth/features/2014/11/hindu-right-ideology-indian-textbooks-gujarat-20141147028501733.html.

133. Sharma, Radha; "Saffronisation of education in Gujarat," The Times of India, 1 September 2001 http://timesofindia.indiatimes.com/city/ahmedabad/Saffronisation-of-education-in-Gujarat/articleshow/1622570533.cms AND "India's Hindu Fundamentalists: People & Power investigates India's Hindu fundamentalists and their influence on the country's government," AlJazeera [People & Power], 08 October 2015 http://www.aljazeera.com/programmes/peopleandpower/2015/10/indias-hindu-fundamentalists-151008073418225.html

134. Wilkes T. Modi in a spin as he replaces Gandhi as face of India's homespun cotton", Reuters (Thomson- Reuters), 13 January 2017 https://www.reuters.com/article/us-india-modi-gandhi/modi-in-a-spin-as-he-replaces-gandhi-as-face-of-indias-homespun-cotton-idUSKBN14X1ES.

135. "Modi makes no mention of Nehru," Deccan Herald News Service, New Delhi, 10 August 2017 http://www.deccanherald.com/content/627339/modi-makes-no-mention-nehru.html AND "In Lok Sabha address, PM Modi omits Jawaharlal Nehru; Sonia Gandhi takes a dig at RSS," Hindustan Times, 09 August 2017. http://www.hindustantimes.com/india-news/pm-modi-echoes-mahatma-gandhi-s-do-or-die-slogan-calls-to-end-poverty-illiteracy-corruption/story-NJIglmYi71vKZD5b2rY6IK.html.

136. Mohanty D. PM Modi takes swipe at Nehru-Gandhi families: Freedom struggle sacrifice of several not few – PM Modi said: "The rebellion against the British in our country the freedom struggle was limited to a few families…" The Indian Express, 16 April 2017 http://indianexpress.com/article/india/narendra-modi-odisha-freedom-struggle-nehru-gandhi-family-4615168/

137. Emperor Ashoka aggressively promoted diversity among his subjects. He also promoted the "energetic practice of the sociomoral virtues of honesty, truthfulness, compassion, mercifulness, benevolence, nonviolence, considerate behaviour toward all…" Moreover, Ashoka encouraged the development of a sense of respect for religious diversity and established religious freedom and freedom of worship, while urging his subjects to make every effort to the "increase of their inner worthiness." – Chandra Sen, Amulya; "Ashoka, Emperor of India," Encyclopædia Britannica, 2017 https://www.britannica.com/biography/Ashoka.

138. In "Ashoka: The Search for India's Lost Emperor," Charles Allen stated, "[w]hen Nehru became a more modern father of the nation as independent India's first Prime Minister, he selected as the symbols of the new India two images directly linked to Emperor Ashoka: the twenty-four-spoked wheel known as the chakra, or 'Wheel of Law', which was set at the centre of the Indian tricolour; and, for its national emblem, the Ashokan capital excavated at Sarnath in 1904–5 showing four lions standing guard over four chakras, representing the 'lion's roar of the Buddha' spreading to the cardinal directions. These symbols were expressly chosen to represent the new, secular India, free of any specific religious affiliation, as the author and journalist Gita Mehta remembers: 'As children, we were often told by our parents that these 2300-year-old symbols were not mere deference to antiquity; they were to inspire us to create a country governed by righteousness.'" – Allen, Charles; "Ashoka: The Search for India's Lost Emperor," Little Brown Book Group/Hachette, London, UK., 2012.

139. Jha S. "Reverence, Resistance and Politics of Seeing the Indian National Flag," Cambridge University Press, New Delhi, India, 2016.

140. "The Rising Tide of Intolerance in Narendra Modi's India," Kennedy School Review - Kennedy School of Government, Harvard University, Boston, MA., 27 July 2016 http://harvardkennedyschoolreview.com/the-rising-tide-of-intolerance-in-narendra-modis-india/.

141. Madhav R. Coming full circle at 70 – Independence Day 2017: For the first time after independence, the dominant idea of India is rooted in India's genius," The Indian Express, 15 August 2017 http://indianexpress.com/article/opinion/columns/independence-day-coming-full-circle-at-70-atal-bihari-vajpayee-hamid-ansari-muslims-india-insecure-modi-nehru-4796919/.

142. Varma, Pramod (UIDAI); "Architecting World's Largest Biometric Identity System - Aadhaar Experience", Strata + Hadoop WORLD {Make Data Work} Conference, 15–17 October 2014, New York, NY, USA https://conferences.oreilly.com/strata/stratany2014/public/schedule/detail/36305.

143. *Ibid*.

144. Khera R. The real beneficiary Aadhaar doesn't empower people, only the state, The Indian Express, 2 June 2017 http://indianexpress.com/article/opinion/columns/uidai-aadhaar-card-the-real-beneficiary-4684994/ AND Ghosh, Mohul; "Aadhaar Card Giving Rise To Increasing Online Frauds In India; Should Mobile Wallets Encourage Its Usage?" Trak.In, 5 June 2017 http://trak.in/tags/business/2015/10/08/aadhaar-card-increasing-online-frauds-india-mobile-wallets-usage/ AND Azad, Shivani; "All residents of this village born on January 1, say Aadhaar cards," The Times of India, 27 October 2017 https://timesofindia.indiatimes.com/city/dehradun/all-residents-of-this-village-born-on-january-1-say-aadhaar-cards/articleshow/61254173.cms AND Express News Service; "Aadhaar of 300 people stolen, Rs 40 lakh pension money swindled," The New Indian Express, 28 October 2017 http://www.newindianexpress.com/states/telangana/2017/oct/28/aadhaar-of-300-people-stolen-rs-40-lakh-

pension-money-swindled-1685237.html AND Krishna, Gopal; "Aadhaar unacceptably intrusive," The Tribune, 30 October 2017 http://www.tribuneindia.com/news/comment/aadhaar-unacceptably-intrusive/489210.html.

145. The Centers for Medicare and Medicaid Services made at least US$48 billion in improper payments in 2010 for Medicare services. – "Medicare and Medicaid Fraud, Waste and Abuse: Effective Implementation of Recent Laws and Agency Actions Could Help Reduce Improper Payments," U.S. Government Accountability Office [GAO-11-409T], Washington D.C., 9 March 2011 http://www.gao.gov/new.items/d11409t.pdf AND Medicare expects to make US$41.1 billion in improper payments for 2016. – "Medicare Fee-for-Service 2016 Improper Payments Report – 2016 Improper Payment Rates and Projected Improper Payments by Claim Type (Dollars in Billions), US Health & Human Services, Washington, D.C.

146. Satpathy T. *Supra*, Note 104.

147. The Data Protection Commissioner (IE) v. Facebook Ireland Ltd., and Maximillian Schrems, Judgement To Refer - The High Court (Commercial) [2016 No. 4809 P.], 3 October 2017 https://www.dataprotection.ie/docs/EN/03-10-2017-Irish-High-Court-grants-the-Data-Protection-Commissioner-its-CJEU-referral-in-DPC-v-Facebook-Ireland-and-Maximilian-Schrems/m/1666.htm.

148. Markovits C. The Un-Gandhian Gandhi," Anthem Books (South Asian Studies), London, UK, 2004.

149. Satpathy T. *Supra*, Note 104.

150. *Ibid*.

151. Sidney A. Discourses Concerning Government, *Supra*, note 113.

152. "Teaching and Learning: Achieving quality for all," EFA/Global Monitoring Report, United Nations Educational, Scientific and Cultural Organization (UNESCO), Paris, 2014.

153. *Ibid*.

154. Abraham D, Rao O. [IndiaSpend]; “86% killed in cow-related violence since 2010 are Muslim, 97% attacks after Modi govt came to power,” Hindustan Times 16 July, 2017 http://www.hindustantimes.com/india-news/86-killed-in-cow-related-violence-since-2010-are-muslims-97-attacks-after-modi-govt-came-to-power/story-w9CYOksvgk9joGSSaXgpLO.html.

155. *Ibid*.

156. Biswas S. Is India descending into mob rule? The BBC (India), 26 June 2017 http://www.bbc.com/news/world-asia-india-40402021.

157. Mukerjee M. Churchill's Secret War: The Britsh Empire and The Ravaging of India During World War II. Basic Books/Perseus Book Group, New York, NY, 2010.

158. Warning: Portions or the whole video may be disturbing for viewers. "Man lynched by mob for allegedly carrying beef in Jharkhand," India-TV, YouTube, 29 June 2017 https://www.youtube.com/watch?v=iTezQT5LcGY AND #NotInMyName: Anti-Lynching Movement In India | The Newshour Debate, Times Now, YouTube, 28 June 2017 https://www.youtube.com/watch?v=k0mFR2W3gn8 AND "Was Told They Were Beef-Eaters, Says Man Arrested For Train Lynching," NDTV, YouTube Archive, 24 June 2017 https://www.youtube.com/watch?v=PzoJiCc38ww.

159. "Spate of public lynchings in India: Mob rule the new rule?," France24, YouTube Archive, 24 August 2017. https://www.youtube.com/watch?v=lYB7QGxp9H0.

160. Koshy SM. Kerala RSS Worker's Murder: Data Reveals Record Of Political Killings, NDTV, 04 August 2017 http://www.ndtv.com/kerala-news/kerala-rss-workers-murder-data-reveals-record-of-political-killings-1733728.

161. Farooqui S. Indian Scholar Who Spoke Out Against Idol Worship Is Shot Dead, TIME World, New Delhi, 31 August 2015 http://time.com/4016747/mm-kalburgi-india-murder-rationalist-idol-worship-hindu-nationalism/ AND Staff; "Narendra Dabholkar murder case: A timeline," The Indian Express, New Delhi | Updated: 11 June 2016 http://indianexpress.com/article/india/india-news-india/narendra-dabholkar-murder-case-a-timeline-2847149/ AND Malekar, Anosh; "Darkness at Dawn: The murders of Narendra Dabholkar, Govind Pansare and MM Kalburgi," The Caravan, 1 August 2016 http://www.caravanmagazine.in/reportage/darkness-dawn-dabholkar-pansare-kalburgi

162. Pimputkar S. Not just Gauri Lankesh, these 10 journalists’ killing questions the safety of the profession in India," The Free Press Journal, 7 September 2017 http://www.freepressjournal.in/india/not-just-gauri-lankesh-these-10-journalists-killing-questions-the-safety-of-the-profession-in-india/1133344.

163. Mahatma Gandhi (PYARELAL); "The Last Phase" (Vol. II), Navajivan Publishing House, Ahmedabad, India, 1958.

164. "Commencement Day: A Celebration Before The New Challenges Ahead; Brandeis University: Brennan Urges Vigiliance In Guarding Rights," The New York Times, 19 May 1986 http://www.nytimes.com/1986/05/19/us/commencement-day-celebration-before-new-challenges-ahead-brandeis-university.html.

165. *Ibid*.

166. *Ibid*.

167. *Ibid*.

168. Justice Brennan’s Brandeis University Commencement Address, *Supra*, Note 164.

169. SAMPLE READING: Schiavenza, Matt; "China's Forgotten Liberal Hero: Hu Yaobang, whose death 25 years ago triggered the Tiananmen Square protests, served China in an era of unprecedented openness," The Atlantic, April 2014 https://www.theatlantic.com/international/archive/2014/04/chinas-forgotten-liberal-hero/360722/ AND Luo, Chris; "Online censorship rolled back on 25th anniversary of death of reformist leader – Days after Hu Jintao’s visit to Hu Yaobang’s former home met with a media blackout, Weibo users enjoy near-uncensored opportunity to mourn the death of the famous reformist leader," South China Morning Post (SCMP), Hong Kong, 15 April, 2014, http://www.scmp.com/news/china-insider/article/1482930/online-censorship-rolled-back-25-anniversary-death-reformist.

170. Branigan Tania; "Crackdown in China spreads terror among dissidents – More than 20 people have been detained and others are missing after anonymous calls for 'jasmine revolution'," The Guardian, 31 March 2011 https://www.theguardian.com/world/2011/mar/31/china-crackdown-on-activists-arrests-disappearances.

171. Lim L. The People's Republic of Amnesia: Tiananmen Revisited," Oxford University Press, New York, New York, 2014.

172. For General Informational Purposes Only. Other material information drawn on the SCS project is from Professional and Non-Public sources. "China to build national social credit system," Xinhua/ChinaDaily, 6 May 2014 http://www.chinadaily.com.cn/business/2014-05/06/content_17486630.htm.

173. "The Writings of Thomas Jefferson, Being His Autobiography, Correspondence, Reports, Messages, Addresses and Other Writings Official and Private" [H. A. Washington, Ed.], Vol VII, Taylor & Maury, Washington, D.C., 1854.

174. U.S. Federal Communications Commission, August 2017.

175. *Ibid*.

176. Kennemer Q. Android Billion, Phandroid, 25 June 2014 http://phandroid.com/2014/06/25/android-has-1-billion-active-users-in-the-past-30-days-and-other-interesting-numbers-from-io/.

177. Fry R. Millennials overtake Baby Boomers as America’s largest generation," Pew Research Center, Washington, D.C., 25 April 2016 http://www.pewresearch.org/fact-tank/2016/04/25/millennials-overtake-baby-boomers/.

178. Williams A. Move Over, Millennials, Here Comes Generation Z, The New York Times, 18 September 2015. https://www.nytimes.

com/2015/09/20/fashion/move-over-millennials-here-comes-generation-z.html.

179. VanSlyke T. Digital Natives, Digital Immigrants: Some Thoughts from the Generation Gap. The Technology Source, May/June 2003 http://www.technologysource.org/article/digital_natives_digital_immigrants/.

180. Delany III, JJ, Governo DM, Noffsinger M. The Generation X and Y Factors (Modern Jury Dynamics ), For The Defense – Toxic Torts and Environmental Law, January 2013.

181. Mobile Mindset Study [Harris Interactive], Lookout, San Francisco, CA, USA June 2012 https://www.mylookout.com/resources/reports/mobile-mindset

182. "The Extended iSelf: The Impact of iPhone Separation on Cognition, Emotion, and Physiology," Journal of Computer-Mediated Communication, Volume 20, Issue 2, March 2015.

183. Mobile Mindset Study, *Supra*, Note 181.

184. Belic D. Tomi Ahonen: Average users looks at their phone 150 times a day!, INTOMOBILE, 9 February 2012 http://www.intomobile.com/2012/02/09/tomi-ahonen-average-users-looks-their-phone-150-times-day/.

185. Altmann EM, Trafton JG, Hambrick DZ. Momentary Interruptions Can Derail the Train of Thought, Journal of Experimental Psychology, Vol. 143, No. 1, 2014.

186. Mark G, Gudith D, Klocke U. The Cost of Interrupted Work: More Speed and Stress, CHI '08 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Florence, Italy — April 05–10, 2008 (ACM).

187. "International Trends in Cybersecurity," Computing Technology Industry Association (CompTIA), Downers Grove, IL., April 2016 AND Liginlal, Divakaran; Sim, Inkook and Khansa, Lara; "How Significant is Human Error As A Cause of Privacy Breaches? An Empirical Study and A Framework For Error Management," Computers & Security, Vol. 28, No. 3, 2009.

188. Nikravan L, Grasz J. (CareerBuilder PoCs), "New CareerBuilder Survey Reveals How Much Smartphones Are Sapping Productivity at Work: 3 in 4 Employers Say Two or More Hours a Day are Lost in Productivity Because Employees are Distracted, " CareerBuilder/Harris, June 9, 2016 http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=6%2F9%2F2016&id=pr954&ed=12%2F31%2F2016 AND https://hiring-assets.careerbuilder.com/media/attachments/careerbuilder-original-2352.jpg?1465224437.

189. "When Worlds Collide the Rise of Social Media for Professional & Personal Use" Kelly Global Workforce Index (KWGI) [RDA Group, Bloomfield Hills, MI], Troy, Michigan, USA June 2012.

190. Fishbein J. Deconstructing digital desires Student Internet use raises questions regarding social media's addictive nature, The Queen's Journal (Queens University, Kingston, ON), 10 February 2012 http://www.queensjournal.ca/story/2012-02-10/deconstructing-digital-desires/.

191. Argumosa-Villar L, Boada-Grau J, Vigil-Colet A. Exploratory Investigation of Theoretical Predictors of Nomophobia Using the Mobile Phone Involvement Questionnaire (MPIQ)" Journal of Adolescence, Volume 56, April 2017.

192. Laconi S, Vigouroux M, Lafuente C, Chabrol H. Problematic Internet Use, Psychopathology, Personality, Defense and Doping, Computers in Human Behavior, Volume 73, August 2017.

193. Dong G, Wang L, Du X, Potenza MN. Gaming Increases Craving to Gaming-Related Stimuli in Individuals With Internet Gaming Disorder, Biological Psychiatry: Cognitive Neuroscience and Neuroimaging, Volume 2, Issue 5, July 2017.

194. Munno D, Cappellin F, Saroldi M, Bechon E, Zullo G. Internet Addiction Disorder: Personality Characteristics and Risk of Pathological Overuse in Adolescents, Psychiatry Research, Volume 248, February 2017.

195. Przybylski AK, Murayama K, DeHaan CR, Gladwell V. Motivational, Emotional, and Behavioral Correlates of Fear Of Missing Out, Computers in Human Behavior, Volume 29, Issue 4, July 2013.

196. Christakis DA. Internet addiction: a 21st Century Epidemic?, BMC-Medicine, Vol. 8, 2010.

197. Tinker B. Four Beds Ready To Treat Internet Addicts," CNN, 7 September 2013 http://www.cnn.com/2013/09/07/health/internet-addiction-treatment-center/.

198. Brown V. The Digital Addiction That Has Teens Wearing Nappies So They Don't Need A Toilet Break – CHINESE Teenagers' Addiction To Technology is So Out of Control, Desperate Parents Are Resorting To Extreme Measures, News, NSW, Australia, 8 June 2016 http://www.news.com.au/lifestyle/health/health-problems/the-digital-addiction-that-has———teens-wearing-nappies-so-they-dont-need-a-toilet-break/news-story/5e0d321846a93337dc9f0260fc0ffc23.

199. Mathews, *Supra*, Note 32.

200. Christakis, *Supra*, Note 196.

201. "Drugs and Alcohol in the Workplace," National Council on Alcohol and Drug Dependence (NCADD), New York, New York, 26 April 2015 https://www.ncadd.org/about-addiction/addiction-update/drugs-and-alcohol-in-the-workplace.

202. *Ibid*.

203. Whitler K. Why More Firms Need A Social Media Governance Plan," Forbes, 14 May 2017 https://www.forbes.com/sites/kimberlywhitler/2017/05/14/why-more-firms-need-a-social-media-governance-plan/#5dd8ea797a2b AND "In 2013, 43% of companies identified internal social media education as a top social business priority, while only 38% indicate having such a program in place, or in progress." – Li, Charlene et. al; "Social Media Education for Employees: Reduce Social Media Risk and Activate Employee Advocacy for Scale — How Leading Companies Prepare Employees for Social Media Success," Altimeter/Prophet, Atlanta, GA, 5 December 2013.

204. Hamilton A, Madison J, Jay J. The Federalist on The New Constitution Written In The Year 1788″ (Federalist Papers No: 55, 6th Edition), R. Wilson DeSilver, Philadelphia, PA 1847.

205. Viseu A et. al. Situating Privacy Online: Complex Perceptions and Everyday Practices, Information, Communication & Society. Vol. 7, Issue 1, 2004 http://www.tandfonline.com/doi/abs/10.1080/1369118042000208924?journalCode=rics20.

206. Greenfield D. Psychological characteristics of compulsive Internet use: A preliminary analysis," CyberPsychology & Behavior, Vol. 2, No. 5, 1999.

207. Toronto E. Time Out of Mind: Dissociation in the Virtual World," Psychoanalytic Psychology, Vol. 26, No. 2, 2009.

208. Suler J. The Online Disinhibition Effect," CyberPsychology & Behavior, Vol. 7, No. 3, 2004.

209. Cooper A et. al. Sexuality and the Internet: The Next Sexual Revolution" In: "Psychological Perspectives on Human Sexuality: A Research Based Approach" [Lenore T. Szuchman & Frank Muscarella (Eds.)], John Wiley & Sons, New York, NY., 2000.

210. Zhou Z et. al. An Error-Related Negativity Potential Investigation of Response Monitoring Function in Individuals with Internet Addiction Disorder," In: "Cognitive Deficits in Schizophrenia and other Neuropsychiatric Disorders: Convergence of Preclinical and Clinical Evidence" [Stuchlik, A., and Sumiyoshi, T., Eds.], Frontiers Media, Lausanne, CH., 2015.

211. *Ibid*.

212. Meeker M. Internet Trends, Kleiner-Perkins, Menlo Park, CA, 31 May, 2017.

213. GSMA "The Mobile Economy," London, UK, February 2017 https://www.gsmaintelligence.com/research/?file=9e927fd6896724e7b26f33f61db5b9d5&download.

214. Worldwide Social Network Users: eMarketer's Estimates and Forecast for 2016–2021, July 12, 2017 https://www.emarketer.com/Report/Worldwide-Social-Network-Users-eMarketers-Estimates-Forecast-20162021/2002081.

215. "International Trends in Cybersecurity," *Supra*, Note 187.

216. Fry R. *Supra*, Note 177.

217. Subject Related Sample Reading: Ashworth, M J; "Preserving Knowledge Legacies: Workforce Aging, Turnover and Human Resource Issues in The US Electric Power Industry," International Journal of Human Resource Management, Vol. 17, Issue 9, 2006.

218. "Millennials Don't Stand A Chance" [Moderator: John Donvan], Films for the Humanities & Sciences (Firm); Intelligence Squared US, New York, NY., 2014 https://www.intelligencesquaredus.org/debates/millennials-dont-stand-chance.

219. Tulgan B. Developing the Next Generation of Leaders," Society of Human Resource Management (SHRM), 4 March 2017.

220. Stempel J. Yahoo Must Face Litigation by Data Breach Victims," NASDAQ, August 31, 2017 http://www.nasdaq.com/article/yahoo-must-face-litigation-by-data-breach-victims-20170831-00786 AND Sook Kim, Queena; "Yahoo! May Be Done, But Its Culture Lives On" [The California Report], KQED News - Los Angeles, 17 June 2017 https://ww2.kqed.org/news/2017/06/17/yahoo-may-be-done-but-its-culture-lives-on/.

221. Parris R. Yahoo Hack: Three Billion Accounts Affected – Every Yahoo User Account Ever Created Has Been Compromised By Huge Data Breach, " WHICH?", 4 October 2017. http://www.which.co.uk/news/2017/10/yahoo-hack-three-billion-accounts-affected/.

222. Moar J. The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation," Juniper Research, 24 April 2017.

223. Kulesa P. Decode The Human Threat: Driving A Cyber-Savvy Culture To Combat Cyber Threats [Human Element & Risk Culture Survey], Willis Tower Watson (WTW), New York, NY, 2017.

224. Yahoo! leadership under Carol Bartz, and Marissa Mayer spread many toxic personal characteristics through the company ranks. For example, see: Kamer, Foster;"F—," Carol Bartz: A Brief History of Yahoo's Ousted CEO and Bad Words," Observer, 8 September 2011 http://observer.com/2011/09/fuck-carol-bartz-a-brief-history-of-yahoos-ousted-ceo-and-bad-words/ AND James, Geoffrey J; "Marissa Mayer's Top 10 Leadership Mistakes – The Yahoo CEO has lost the confidence of employees and investors alike. Here are the common management mistakes she should have avoided," INC., 10 January 2016 https://www.inc.com/geoffrey-james/top-10-management-mistakes-marissa-mayer-made.html AND Bradt, George; "How To Avoid Yahoo's Performance Management System Rigging Debacle," Forbes, 2 February 2017 https://www.forbes.com/sites/georgebradt/2016/02/02/how-to-avoid-yahoos-performance-management-system-rigging-debacle/#7e049d6bb8d9.

225. Associated Press Staff; "Yahoo punishes CEO Marissa Mayer over hacks that cost firm $350 million," The Telegraph (Technology) [UK], 2 March 2017 http://www.telegraph.co.uk/technology/2017/03/02/yahoo-punishes-ceo-marissa-mayer-hacks-cost-firm-350-million/.

226. Kobie N, Betteridge I. Yahoo confirms it lost 500m account details in “state-sponsored” attack – Several hundred million accounts exposed as Yahoo is set to finalise deal with Verizon, alphr, 23 September 2016 http://www.alphr.com/yahoo/1004383/yahoo-confirms-it-lost-500m-account-details-in-state-sponsored-attack.

227. Kulesa P. Decode The Human Threat: Driving A Cyber-Savvy Culture To Combat Cyber Threats [Human Element & Risk Culture Survey], Willis Tower Watson, New York, NY, 2017 (emphasis not in the original).

228. Bradley N. et. al. 2016 Cyber Security Intelligence Index" (IBM X-Force ® Research), IBM Security, Somers, NY, 2016.

229. Ornstein C. Inappropriate Social Media Posts by Nursing Home Workers, Detailed," ProPublica, 21 December 2015 https://www.propublica.org/article/inappropriate-social-media-posts-by-nursing-home-workers-detailed AND Mathews, *Supra* note 32 AND Clark, James; "Navy nurse (sic) flips newborn the finger, calls baby 'mini Satan' on Snapchat," Business Insider, 20 September, 2017. http://www.businessinsider.com/navy-nurse-flips-newborn-the-finger-calls-baby-satan-on-snapchat-2017-9.

230. The names, social security numbers, birth dates, addresses and, in some cases, driver’s license numbers and credit cards numbers of people were compromised. Solon, Olivia; "Credit firm Equifax says 143m Americans' social security numbers exposed in hack, " The Guardian [UK], 7 September 2017 https://www.theguardian.com/us-news/2017/sep/07/equifax-credit-breach-hack-social-security.

231. Melin A. Three Equifax Managers Sold Stock Before Cyber Hack Revealed," Bloomberg, 7 September 2017. https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack.

232. Hopkins N. Deloitte hit by cyber-attack revealing clients’ secret emails – Exclusive: hackers may have accessed usernames, passwords and personal details of top accountancy firm’s blue-chip clients, The Guardian [UK], 25 September 2017 https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails.

233. *Ibid*.

234. "State of Cybersecurity: Implications for 2016" (An ISACA and RSA Conference Survey), ISACA, Rolling Meadows, IL, USA, 2016.

235. "State of Cyber Security 2017 Part 2: Current Trends in the Threat Landscape," ISACA, Rolling Meadows, IL, USA, 2017.

236. "Beyond the General Data Protection Regulation (GDPR): Data Residency Insights from Around the World," McAfee [Vanson Bourne], Santa Clara, CA, October 2017.

237. "State of Cyber Security 2017 Part 1: Current Trends in Workforce Development," ISACA, Rolling Meadows, IL, USA, 2017.

238. "Keeping a Lock on Privacy: How Enterprises Are Managing Their Privacy Function," ISACA, Rolling Meadows, IL, September 2015.

239. *Ibid*.

240. Mathews, *Supra*, Note 32.

241. Alvarez M, Bradley N. et. al. Index 2017: The Year of The Mega Breach," IBM X-Force Threat Research, IBM Security, Somers, NY, 2017.

242. Internet Security Threat Report (ISTR) - 2017, Vol. 22, Symantec, Mountain View, CA, April 2017.

243. Kessem L. Ransomware: How consumers and Businesses Value Their Data," IBM Security, Somers, NY, 2016.

244. Internet Security Threat Report (ISTR) – 2017, *Supra*, Note 242.

245. 2016 State of Cybersecurity in Small & Medium-Sized Businesses (SMB), Ponemon Institute [Keeper Security Commissioned], Traverse City, MI, June 261.

246. Stinson S, Dawson DA et al. Prevalence, Correlates, Disability, and Comorbidity of DSM-IV Narcissistic Personality Disorder: Results from the Wave 2 National Epidemiologic Survey on Alcohol and Related Conditions, Journal of Clinical Psychiatry, Vol. 69, Issue 7, July 2008.

247. *Ibid*.

248. Twenge, Jean M and Konrath, Sara et al; "Egos Inflating Over Time: A Cross-Temporal Meta-Analysis of the Narcissistic Personality Inventory," Journal of Personality, Vol. 76, No. 4, August 2008.

249. Twenge JM, Campbell WK. Narcissism Epidemic: Living in the Age of Entitlement,” Free Press, New York, NY, 2009.

250. Vazire S, Funder DC. Impulsivity and the Self-Defeating Behavior of Narcissists," Personality and Social Psychology Review, Vol. 10, No. 2, 2006.
251. Allen BJ. Diversity and Organizational Communication," Journal of Applied Communication Research, Vol. 23, Issue 2, 1995.
252. Sample Reading Only: Hill, Ronald P; "Managing Across Generations In The 21st Century: Important Lessons From the Ivory Trenches, Journal of Management Inquiry, Vol 11, Issue 1, 2002.
253. Bergman SM et. al. Millennials, Narcissism, and Social Networking: What Narcissists Do on Social Networking Sites and Why, Personality and Individual Differences, Vol. 50, Issue 5, 2011.
254. *Ibid*.
255. "How Millennials Want to Work and Live," Gallup Research, Gallup Research, Washington, D.C., 2016. http://www.gallup.com/businessjournal/191459/millennials-job-hopping-generation.aspx.
256. *Ibid*.
257. *Ibid*.
258. Rouland C. Will Millennials Be The Death Of Data Security?, DARKReading, 27 January 2015 https://www.darkreading.com/operations/wiil-millennials-be-the-death-of-data-security-/a/d-id/1318806.
259. Sample Reading Only: Mehta, Jal; "Why American Education Fails And How Lessons From Abroad Could Improve It," Foreign Affairs, May/June 2013 https://www.foreignaffairs.com/articles/united-states/2013-04-03/why-american-education-fails AND Robinson, Gerard and Scafidi, Benjamin; "More Money, Same Problems: Showering public schools with funds has been a costly failure. Why not try something new?" US News & World Report, 20 September 2016 https://www.usnews.com/opinion/articles/2016-09-20/more-money-wont-fix-failing-public-schools.
260. "The Definitive Guide to Building a Better Workforce – Lessons from Best-in-Class Companies on Recruiting and Retaining Elite Talent," Adecco - Aberdeen, February 2016.
261. Rojstaczer S. Where All Grades Are Above Average, The Washington Post, 28 January 2003 https://www.washingtonpost.com/archive/opinions/2003/01/28/where-all-grades-are-above-average/8f7629fd-f74f-46c7-8187-419c31487cb9/ AND "Grade Inflation at American Colleges and Universities," 29 March 2016 http://www.gradeinflation.com/.
262. Mathews R. Presentation to the Special Session of IFMBE - Global Citizen Safety & Security Working Group, "Privacy, Safety & Security: Pathways To Preserve Your Rights In Interoperable Global Healthcare Venues," IUPESM World Congress 2015, 11 June, 2015.
263. *Ibid*.
264. *Ibid*.
265. Hunter, Jane; "Israeli Foreign Policy: South Africa & Central America," *Supra*, Note 87.
266. Complaint Filed: Hadiyah Charles v The City of New York, Raymond Kelly, Pamela Benites, Raymond Williams and John Doe [CV12 6180], United States District Court - Eastern District of New York, New York, New York, 17 December 2012.
267. Stinson Sr. Philip M et. al. Police Integrity Lost: A Study of Law Enforcement Officers Arrested" (Final Technical Report)[Research Performed Under Grant Award Number: 2011-IJ-CX-0024, Office of Justice Program-U.S. Department of Justice], Bowling Green State University, January 2016.
268. Weisburd D et. al. The Abuse of Police Authority: A National Study of Police Officers' Attitudes [Research Performed With Support from Grant Number 97–CK–WX–0047 - US Department of Justice], The Police Foundation, Washington, D.C., 2001.
269. Dorfman DN. Proving the Lie: Litigating Police Credibility, American Journal of Criminal Law, Vol. 26, 1999.
270. *Ibid*.
271. Wilson MD. An Exclusionary Rule for Police Lies, American Criminal Law Review, Vol. 47, No. 1, 2010.
272. Weisburd D. et. al. The Abuse of Police Authority," *Supra*, Note 268.
273. Para 38, Amended Complaint and Demand for Jury Trial in: "Ruben An v The City of New York [Civil Case No.: 16 Civ. 05381 (LGS)], United States District Court - Southern District of New York, New York, New York, 23 February 2017.
274. "David Floyd, Lalit Clarkson, Deon Dennis and David Ourlicht, Individually and on Behalf of a Class of All Others Similarly Situated v. The City of New York" (Opinion & Order 08 Civ. 1034 (SAS)), United States District Court - Southern District of New York, New York, New York, 12 August 2013.
275. *Ibid*.
276. Voreacos D, Weinberg N. Senator Menendez Juror Asks Trial Judge, 'What Is a Senator?', Bloomberg, November 7, 2017 https://www.bloomberg.com/news/articles/2017-11-07/senator-menendez-juror-asks-trial-judge-what-is-a-senator.
277. Putnam RD. Bowling Alone - The Collapse and Revival of American Community," Simon & Schuster, New York, New York, 2000.
278. "Why we need to teach geography, Tonight Show/NBC, YouTube Archive, https://www.youtube.com/watch?v=7_pw8duzGUg AND "JayWalking Citizenship Test," Tonight Show/NBC, YouTube Archive, 11 December 2014 https://www.youtube.com/watch?v=WJlY9C7YWzI.
279. "Quality Counts: A Report Card on the Condition of Public Education in the 50 States" [Ronald A. Wolk, Ed.], Education Week, Washington, D.C., 1997 Cited In: Putnam, Robert D; "Bowling Alone - The Collapse and Revival of American Community," Simon & Schuster, New York, New York, 2000.
280. "Americans Are Poorly Informed About Basic Constitutional Provisions," Annenberg Public Policy Center (APPC) - University of Pennsylvania, Philadelphia, PA, USA 12 September 2017 https://www.annenbergpublicpolicycenter.org/americans-are-poorly-informed-about-basic-constitutional-provisions.
281. *Ibid*.
282. "Well Known: Twitter; Little Known: John Roberts, An Overview, " Pew Research Center - US Politics & Policy (Pew Charitable Trusts), Washington, D.C., 2010 http://www.people-press.org/2010/07/15/well-known-twitter-little-known-john-roberts/
283. Justice Brennan's Brandeis University Commencement Address, *Supra*, Note 164.