Health Technol. (2017) 7:377–388
DOI 10.1007/s12553-017-0196-0

ORIGINAL PAPER

Reflections upon periclitations in privacy: perspectives from Rwanda's digital transformation

Jean Philbert Nsengimana[1]

Received: 29 August 2016 / Accepted: 12 May 2017 / Published online: 12 July 2017

Abstract The Information and Communication Technology (ICT) revolution has brought considerable socio-economic benefits to humanity over the last 50 years. However, one of its side effects has been an increased threat to personal privacy owing to the widespread use of digital services that make utility of personal information, the extreme ease with which that information is captured, transmitted, analyzed and stored coupled with the incentives for a range of actors to misuse the information at their disposal or reach. This article presents a ministerial view that one should not have to trade-off between privacy and security, or be told to give-up privacy for safety. In part, this declaration is foundationally germane to Rwanda's digital transformation, and our society's approach to erecting Privacy protections, harnessing the deep value that Privacy had once held in Rwanda's pre-colonial tradition, and has again, in her most recent history. In view of a rapid transformation that is presently turning the country into a digital hub for the Continent of Africa, Rwanda is charting a path forward to achieve a double purpose; on one hand the prospect of leveraging information technology for the benefits of her citizens, and on the other hand, securing and protecting the privacy of her citizens, as a key component of Rwanda's societal identity. This article further presents that given the leadership that Rwanda has demonstrated in Information and Communication Technology (ICT) for Development in Africa, the nation's course of action in relation to data and personal privacy protection will have a positive influence on the rest of the African continent that is now bracing to form a single digital market through the Continent-wide Smart Africa initiative.

Keywords Privacy · Security · Data protection · Rwanda · Smart Africa · Digital transformation

1 Introduction

The advances in information and communication technologies over the last five decades, have caused a profound transformation in how individuals, communities and entire nations live, learn and work. These changes have been so significant, and so much so, that global societies needed to consider the collective intersection of changes as initiating a shift, from the second, to the third industrial revolution. The first industrial revolution was marked by the introduction of mechanical production, enabled by the steam engine during the second half of the eighteenth century. That shift ended the agrarian revolution, which had been in place for more than ten thousand years; with a production mode based on human and animal muscle power. The second industrial revolution was ushered by the advent of electricity and it enabled further improvements in mass production. The third revolution often referred to as the digital revolution was born as a product of the 1960s, and it was enabled by the development of semiconductors, mainframe computing, parallel processing, personal computing and Internet. Today, the world is at the brink of yet another revolution, the 4th, driven by a rapid convergence of technologies across the biological, physical and multiple digital domains [1].

Rwanda is not isolated from these world transforms. As part of her *vision 2020* [2], Rwanda is undergoing a massive

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

✉ Jean Philbert Nsengimana
nsengimanajp@gmail.com; http://www.myict.gov.rw/home/

[1] Ministry of Youth & Information & Communications Technology (MYICT), Pension Plaza, KN 3 Rd, Kigali, Republic of Rwanda

digital transformation, aimed at moving the economy and society from a subsistence agriculture base, to an information and technology hub for the region and the continent. This transformation pathway, in Rwanda's case, will permit her to almost leapfrog the second industrial evolution - to position the country firmly in the third industrial age, while aspiring to be among the leaders of the fourth. One of the side effects of rapid digitization in the economy has been the increased threat to people's privacy, driven by the extreme ease with which private information is in present times captured, exchanged, used and maintained. Coupled with the existence of enormous economic and other malicious incentives for a range of actors to unlawfully access and misuse personal information, it became an imperative for the Rwandan Government - to take measures that would ensure the sanctity of privacy in world where is an ever increasing demand to digitize information. Given such considerations therefore, article 23 and 38 of Rwanda's constitution have enshrined privacy as a constitutional right, which is linked to the person's honor and dignity [3]. The Government has, and continues to put in place, number of policies [4], legal [5], regulatory, institutional and technical instruments in place to ensure that personal information and privacy shall remain protected, and that any infringement thereof is met with appropriate consequences [6] (relating to the Code of Criminal Procedure).

2 Privacy: the Rwandan context

2.1 The pre-colonial Rwanda

Historically, Rwandans have accorded great significance and importance to the societal value of privacy. In a society where oral communication was the main way to transmit information, it was highly dishonorable act to publicize or otherwise make common, any detail regarding 'self,' one's family or others in a variety of contexts. Children were taught at a very young age to refrain from saying, what they ate at home, describe the whereabouts of their parents, or recounting any conversation they may have heard from adults. In fact as a measure of precaution, children were always dismissed from places where grown-ups would gather and have certain conversations. Several social relations required even higher levels of privacy. For example, within *in-law* relations, parties had to observe strict behaviors such that none would invade the privacy of *parents-in-law,* even accidentally. Strangers were untrusted by default, and were not allowed to be party to any information related to the environment they found themselves within, until some basic level of trust had been established. Still, being party to communications, or otherwise available privileged information beyond the establishment of trust, did not mean that any such information heard could be repeated, anywhere. Privacy of community or political leaders or elders was strictly protected by those around them. No information about the former's personal activities, health conditions, or social relations was to be shared. Information about personal property was also protected. Cows were the main form of wealth accumulation, and it was strictly prohibited to count a person's cows, and, or to tell of that count to anyone.

2.2 The post-colonial Rwanda and 1994 genocide against the Tutsi

Privacy, as understood by Rwandans was dealt a great blow by many aspects of colonialism. First, it was shattered by the culture clash that accompanied colonialism, which was further exacerbated by the nature and compositions of colonial administrations, and the introduction of Christianity into the region. Pre-existing 'social taboos,' which included a great deal of personal privacy protection dimensions were destroyed by the spread of Christianity. Agents of the Catholic Church gave blanket absolutions for those Rwandan people who violated their 'traditions' such as Privacy Protections. Thereafter, a common Rwandan adage emerged, which said: *"Kiliziya yakuye kirazira",* translated roughly, it suggested: *"the church killed all taboos".* As an example, one of the taboo's that was widely disregarded or violated was that people's cows could now be counted publically - to levy tax, and, or categorize people into social classes and ethnic origins; an act – for which, the Church delivered absolution. Another was the introduction of mandatory identity cards for all citizens 18 years of age, and above, which detailed their ethnic origins. Indeed, some roots of the 1994 Genocide against the Tutsi can be traced to a stage in Rwanda's history of the 1920s. The forced classification of people into income classes, further segregated by ethnic groups, was subsequently used to 'divide and to rule' [7] the society. This malicious set-up was unremittingly and heartlessly exploited by successive generations of colonial, and post-colonial leaders, which then became a strong constituting and foundational component to the genocide ideology [7]. With the introdion of writing as an increasingly important form of communication in Rwanda, since the beginning of the twentieth century, privacy practices shaped by the oral traditions came under a new threat. The information that would be known by only a few, such as certain royal rituals, was openly disclosed and published [8].

3 The global dash to a hyper connected society: a ministerial view

Today, privacy has come under a different, perhaps more powerful force: ICT. The extreme convenience that technology has provided to many daily routines, in exchange for people's private information has already put privacy in jeopardy at a large scale on several highly publicized occasions. The

digitalization of the many aspects of human lifestyles and their respective compartments, and, or components have gone beyond a 'non-return' point. Indeed, a growing range of vital services today are provided as "digital by default" [9]. For Example, today, business registration in Rwanda can only be done online.[1] Governments and private service providers are working to provide a seamless digital experience from "the cradle to the grave". The digital identity that is assigned at birth, or is subsequently acquired through one's own volition, and with one's first account on a "connected system" – whether it is in the form of an email or bank account, generates a foot print, that keeps growing – with associated services and transactions. Over time, the amount of information in one's digital footprint processed through increasingly powerful machine learning, targeted data mining algorithms and artificial intelligence systems, is potentially able to be turned into a powerful lens, providing deep-insights into one's life that can be used for *the good, the bad or regrettably*, *the ugly*. This is true for individuals, entire communities and nations. The good use of digital identities include the responsible and constructive use of personal information by Governments, for example, to provide personalized effective, reliable and highly efficient experiences across multiple domains including healthcare, education, business and leisure. The *bad use* ranges from the careless handling of personal data by its custodians, to the malicious exploitation of personal information for the economic gain of various parties. Misuse of personal information shifts to the realm of *ugliness* when it is used to assail the existence and maintenance of basic human rights, societal cohesion, and stability.

A higher degree of personal awareness - related to the risks to privacy, exercising deliberate personal diligence and the existence of a good deal of technical competence is necessary to deliver the *good* - while preventing the *bad* and *ugly* from taking hold. Indeed, the dignity of people whose lives have been saved through telemedicine for example, can be jeopardized, if their digital health records and sensitive genealogical and other genetic data – were to fall into the hands of ruthless people. The delivery of a Government and governance systems that is self-service, available on 24/7 basis, and able to respond to citizen's requests in real time from a variety of connected smart devices, has pushed the limits of convenience, safety, security, reliability and accountability, all of which are invaluable ingredients to the conservation of democratic values. Such transformational experience requires however, the digitization and integration, and the maintenance of such matters as people's identity, property information, civil and fiscal status. In this context, the trust between the people and governments that hold such vital information about their respective citizens need to be irreproachable. Lack of such trust and alternative recourse would be equivalent to the people being taken hostage, or being digitally colonized by whoever has access to their private data against their will. The consequences of the misuse of such vast amount of information upon personal dignity, and, social and national order could only be termed as immense. The constructive human relationships initiated and maintained though social media platforms has enriched lives in a measure only evidenced by the widespread and rapid adoption of such platforms. Many of the "free" social networks and other online services such as instant messaging, banking, even education and entertainment, require that users submit personal information, for example, into "a cloud" that is supposed to be protected by the service provider. The collection of technologies called as the Internet of Things (IoT) is increasingly finding way into our houses, cars, farms, workplaces, and even our bodies. The network of CCTVs[2] in city's security sensitive locations, public transport, hotels and other public spaces is being expanded to ensure people's safety and further national security aims. The word "Smart" that is supposed to mean: instrumented, interconnected and intelligent [10] – can be found being applied routinely to almost everything: from entire cities to communities in rural areas, from schools to hospitals, from cars to household items, and even living organisms such as cows. The principle and intent of connecting everything is perhaps a noble goal: remote monitoring of a patient – to save lives, climatic controls in a greenhouse farm for increasing food security, energy consumption optimization for buildings and entire cities to reduce their carbon footprint in an effort to keep global warming in check, self-driving cars to reduce traffic accidents, etc. Indeed, given the momentum that the mobile industry and broadband internet connectivity [11] has taken, as well as the IoT industry [12], it can be safely assumed that it is only a matter for time before everyone and everything that can be connected - will be connected.

The question, for not only Rwanda, but also the world, remains whether sufficient awareness of the risks associated with such hyper-connectivity poses to personal and societal privacy exists, and the necessary respective protections have been built to ensure that the public is appropriately safeguarded.

[1] "Your step-by-step guide to investment related procedures in Rwanda," Business Registration - E-Guide from Government of Rwanda, Business Facilitation Programme - United Nations Conference on Trade and Development (UNCTAD), 2017 http://businessprocedures.rdb.rw/menu/1?l=en

[2] Closed Circuit Television

And, as it has been proven many times, custodians of data repositories have not been forthright with respect to a divulgence of information (Sean [13]), diligent in their efforts to protect [14], and are in many instances plainly delinquent in general practices to be secure [15]. As it is often said, those conducive circumstances that lead to the occurrences of large-scale breaches poses the question, not of "whether," rather, "when." It has also been said that following the aforementioned statement, it may not be difficult to imagine a future where privacy as it used to be known – could be seen as becoming extinct [16]. Such a course could very well lead to a vastly different type of society, with wholly different set of values, rule and systems of governance, as well as corresponding organizational and operational constructs.

Nevertheless, none of the threats to Privacy should be attributed to technology per se'. The blame should be fairly apportioned across to those who have made, and continue to make, conscious and deliberate decisions to use technology in ways that will permit the invasion of people's privacy. "Ignorance is insufficient as defense" [17]. The reasoning that, the provision of all the excellent uses of technology have to be accompanied by loss of privacy as a trade-off, is a fundamentally flawed presentation. Furthermore, asserting that security cannot be guaranteed without sacrificing people's privacy cannot be justified [18]. Indeed, as much as some technology platforms were intentionally designed to deliver benefits, while putting privacy at stake, the market could provide alternative technologies and, or choices that deliver the same, if not even greater benefits, while ensuring privacy protection [19]. Principally at least, while nations of the world are undergoing states of digital transformation previously thought to be inconceivable, the *'big-ask'* to accept the need, and to then make monumental sacrifices in one's privacy for the sake of security is appercipiently equal to the crusades of argumentors on either side of the "*Dialogue on the Two Chief Systems of the World*." [20].

Accordingly, for the sake of encouraging the build-out of energetic, creative, healthful, productive, stable and a thriving "virtual commons" in our Digital Century, humanity must address the great insufficiency before us in terms of Privacy, that is to identify and disentangle the natural truth from the *"Two Chief Systems of the World"*[3] as presented; and to construct a 'manifest' life and living habitat, where none will ever have to make a trade-off between Privacy, Safety and Security, on account of some circumstance that would impose an unnecessary and definitely harmful requirement to people and communities. Today, this habitat as it is proposed here, by degrees, share, what seems to be an enormous capital similarity to the once contrarian idea of heliocentricism - representing natural truth on one hand, and the dominant theologically backed[4] pre-telescope knowledge of geocentricism on the other [21] Additionally, possessing great awareness to the existence of technologies able to assist in the preservation of privacy while ensuring safety and security; political, business and community' leaders having the necessary courage to investigate and promote much needed technological and paradigmic alternatives, and to act with focus and determination to face market forces threatening to make humanity's privacy history, are now - a must. Privacy: a shared common goal to establish strong social cohesion in Rwanda.

In a country with a recent history of division, and massive human loss, providing Information and Communication Technologies (ICT) as a medium for reconciliation, healing and the linking of families and of communities, was seen as an ideal enabler of social cohesion. The commitment to connect the whole country, and not just the commercially viable urban areas, allowed Rwanda to avoid the common pitfalls of exacerbating income inequalities, gender, and rural/urban divides. Information and Communication Technologies (ICT) thus became an exceedingly handy tool, to advance "post-genocide" Rwanda's key philosophical and sociopolitical foundations – related to the building of an inclusive and people-centered society.

Many of Rwanda's core traditional and cultural values have Privacy as one of the key foundations. The leading foundational value is that of "*agaciro*", only loosely translated as "dignity", but also including elements of self-confidence, respect for self, and for others, as well as freedom. In Rwanda, *agaciro* is only attainable if Personal Privacy is, for oneself and others, respected. From the first paragraph of the constitution, human dignity is defined as a foundational attribute for the Rwandan society of the present and the future, ranked at the same level as security, freedom and justice [3]. Supportingly, the abolition of death penalty - within a post-genocide Rwanda context should be seen as the ultimate demonstration that the State has put respect for life and human dignity above all. Another leading societal value is "*ubupfura,*" or nobility, added to the elements of loyalty and humility, which also places Privacy at the forefront. A person of *ubupfura* – or a noble person, is a sophisticate, and is

[3] With respect to Privacy, the reference to *"Two Chief Systems of the World"* refers to two schools of thought; one (echoed by some of the highest authorities in World Governments) proposes: Security and Safety of populations can only be achieved at the expense of Privacy, while the other proposes: necessary levels of Safety and Security can be achieved - without sacrificing Privacy

[4] Ruling of Cardinal Robert Bellarmine and the 11 Theologians to the Holy Office (under signature of Pope Paul V, to assess heliocentricism) made public on 24 February 1616, that 'heliocentricism' was: "foolish and absurd in philosophy and formally heretical as it expressly contradicts the teachings of Holy Scripture."

therefore, among other things, naturally expected to abstain from invading, or even be seen as trying to invade other people's privacy.

Amidst tumultuous digital transformation, Rwanda is being guided by all that we treasure in our society (in a return to our roots), to not compromise or fail in the maintenance and preservation of such key societal pillars, because the very strength and durability of our present society, and our nation's future are inextricably linked to the survival of such societal pillars.

4 Rwanda's digital transformation journey – a review

The 1994 Genocide against the Tutsi - left Rwanda covered in blood, and in smouldering ashes. The country was on the brink of literally becoming a failed state [22], or worse, disappearing as a nation entirely. On the international stage, the country was vilified and isolated by the same forces that had planned and orchestrated the genocide. Meanwhile, the genocidal regime, operating from the Great Lakes of Africa, a location to which they had been driven into exile, threatened to come back, and attack the country again, to *"finish the job"* – of killing all Tutsis who had survived the genocide, and to annihilate the forces that had stopped it. The "apocalyptic" outcome could have happened, had the forces that stopped genocide and found their own families almost exterminated by their neighbors had opted to carry out revenge killings. It was amidst cries of babies left orphans, thousands of injured to be treated, the dead to be buried, the need to secure and establish homeland security, justice to be rendered amidst chaos and a loss of confidence, and the need for a traumatized nation to heal, that a bold vision was born, from the leadership of the RPF,[5] the movement that had stopped the genocide. Determined not to fail but clearly at crossroads as to how to turn around a deeply wounded society, the leadership counter-intuitively opted to transform the largely agrarian society into a twenty-first Century information society where National Unity and Reconciliation as well as ICT were going to be cornerstones.

By the early 2000, as the country was emerging from the fiery aftermath of the Genocide, a 20 year socio-economic development plan – *vision 2020* - was introduced. In a very counter- intuitive fashion, President Paul Kagame pushed to position ICT at the center of the development strategy. At a time where everything was a priority – from food security to public education, providing healthcare, and justice for genocide survivors and their families, alongside the need to deal with literally hundreds of thousands of genocide perpetrators, every dollar in the national treasury needed to be spent very wisely and cautiously.

The significance of the visionary Presidential prioritization was the recognition that ICT was going to be a significant enabler for all the other sectors, which research would later reveal as being factually important, that there is a strong causal relationship between broadband penetration, and GDP growth of a nation [23].

Rwanda's ICT development journey proceeded through a series of 5 year strategic National Information and Communication Infrastructure (NICI) plans. A condensed representation of that ICT development - in relationship to the conception, development and deployment of Privacy protection instruments for the present and posterity, are immediately presented herein.

NICI I (2001–2005) focused on the liberalization of the Telecommunications Sector and the setting up of legal, regulatory and institutional mechanisms to attract private sector investments and grow the sector. The Rwanda Information Technology Authority (RITA) was established to coordinate the implementation of NICI Plans. In 2001, Rwanda Utilities Regulation Authority (RURA), an independent multi-sectorial Regulator with mandate to regulate the ICT sector was also established. Through its mandate of customer protection of telecommunication sector, RURA was given a pivotal role in enforcing people's right to Privacy in the digital domain.

The second NICI Plan (2006–2010) paved the way for large-scale investment into ICT infrastructure. At a time when most countries in Africa were dependent on satellite Communication for access to the Internet, the Rwandan Government invested into situating 2300 Km of 50 Gbps fiber optic cable, connecting all the 30 Districts of the country, and 9 Border Posts, making it Africa's densest national fiber optic cable backbone network deployment then, in anticipation of connecting to the submarine cables that were being laid adjacent to Africa's East Coast.

While the private sector was initially reluctant at the to invest, citing an unclear business case, investors quickly realized that the move towards digital transformation of Rwanda was unstoppable, and started to invest into installation of their own optical fiber channels and the setting-up of accompanying network infrastructure, bringing the total installed optical fiber cabling to more than 6000 Km today. Today, the backbone in part, is being used as a backhaul for the national 4G LTE network that aims at reaching 95% of the population by end of 2017.

With regard to Privacy, at a very fundamental level, and is presented here only as an example, that the One Laptop Per Child (OLPC - introduced in partnership with MIT Media Lab - into 416 schools across the country to 200,000 students) and the smart classroom programs have been designed to impart Privacy consciousness to young learners from the onset. Prompted by a need to securely share one terminal, by more

[5] Rwanda Patriotic Front

than one student, a unique *"One Digital Identity per Student"* program was implemented. When a student logs on any terminal, they only have access to their private learning workspace, which is intentioned to instill the sense that, in the digital world, everyone deserves their own space that should be respected, and not made accessible to any other person.

The main focus on the third NICI III (2011–2015) plan was on digitizing public services. Up to 100 digital services were developed across the key social and productive sectors of agriculture, education, healthcare, government and financial services. Today, Rwanda has three times more mobile wallets than bank accounts. Mobile wallets are mobile-based identities or accounts used to send and receive payments and access an increasing range of financial services. Between 2011 and 2015, the number of mobile financial subscribers increased more than 10 fold, from about 600,000 subscribers to more than 7.5 million [24]. The use of mobile phones to access financial services in turn accelerated economic growth in many other ways, such as allowing millions of Rwandans to enter and participate in a formal national economy – extending economic opportunities such as encouraging personal and family savings, and providing access to capital and forms of credit to the many who were previously financially excluded. However, the use of mobile wallets has sometimes raised serious security concerns, due to cases of theft that can be orchestrated from inside the mobile network operator organization [25] or through identity theft, based on social engineering and fraudulent SIM (Subscriber Identity Module) registration on which users accounts are based on [26]. The inherent security weaknesses of the SIM technology itself [27, 28] call for a superior technological mechanism to deliver the important digital financial services. One option being explored by the Republic of Rwanda in conjunction with other technologies, is the use of Blockchain, which is able to assure greater security of information, and thereby, better personal privacy also.

With increased penetration of mobile devices and Internet use, the need to provide a stronger framework for protecting personal Privacy, while ensuring that information technology utility does not turn into a threat for national economic security – has become very pressing, and to the forefront of national leadership considerations. The task has been rendered more complex by Interoperability demands in the heterogeneity or convergence of diverse telecommunication systems, hardware and software systems, and many information processing domains/platforms and accompanying support systems.

4.1 The smart Rwanda 2020 master plan (SRMP)

The fourth generation of the national ICT plan was named *Smart Rwanda Master Plan 2020 (SRMP)* [29] and was developed in line with the principles of the Smart Africa Manifesto, endorsed by the seven founding Heads of State of the Smart Africa Alliance. The Masterplan defined the following three key areas of focus:

> **National digital transformation** – the intention is to leverage digital technologies to improve outcomes for the following key social and economic sectors: education, agriculture, healthcare, government services delivery, financial services, trade and industry, youth and women empowerment. Anticipating that massive digitization would inevitably lead to sophisticated implications on data protection and raise privacy concerns the Cabinet ordered that each concerned sector elaborates a specific policy to guide its digital transformation and identifies any legal or regulatory requirements to safeguard information security and people's privacy. In particular, the Health Sector is presently engaged in the development of a framework that is comparable to USA's HIPPA[6] When the e-Health sector policy gets approved within the financial year ending in June 2017, Rwanda will have been among the first African countries to have specific measures in place to assist the advancement of privacy protections, through the deployment of a legislative framework specifically oriented toward the health sector.
> **Innovation and business** - With the aim of becoming an Innovation Hub in the region, Rwanda is building an innovation ecosystem that should result into an environment for African technology startups to flourish and tap into the growing African and global markets for technology enabled goods and services. In anticipation of the increased production and use of personal data by the different applications that the technology companies are going to produce for the pan-African market, Rwanda is currently investing time, energy and financial resources to have in place, the necessary technical, legal and regulatory guideposts and protections, to position the country as a competitive, trustworthy, safe and secure place to host globally produced data. In line with this commitment, Rwanda has invested in a Digital Forensic Laboratory under the Rwanda National Police, a CSIRT[7] and PKI[8] under the Rwanda Information Technology Authority as well as a Regional Internet Exchange (IX), all of which have the vision of enabling the provision of secure digital services. The Digital Forensic Laboratory is developing advanced capabilities to investigate cybercrimes and other technology assisted

[6] Health Insurance Portability and Accountability Act of 1996, USA. It is recognized here that while HIPAA is not a Privacy Law per se,' the act serves as a guidepost to information exchange within healthcare transactions in the United States of America. Rwanda is in the middle of developing such statutes, and it is in such a context, the reference is being made.
[7] Computer Security Incident Response Team
[8] Public Key Infrastructure

crimes such as financial crimes but also illegal access, and the use of private information.

Rwanda's ICT strategy has only been able to advance properly, due to the fact that key aspects of the national vision, and necessary governmental support systems have intrinsically been given great care and attention, internal focus and allocation of valuable and scarce national resources to suitably develop. Rwanda has received praises for her excellent performance in dramatically transforming the national business climate, as evidenced by the World Bank's ***Doing Business*** Index [30], which has ranked Rwanda as the second best place to do business on the African Continent. Rwanda was also ranked by the World Economic Forum Global Information Technology Report as top performer in Africa on the "Government Success in ICT Promotion", "ICT use and Government Efficiency" as well as "Impact of ICT on access to basic services," in such areas as education, healthcare and financial services [31]. Rwanda's success in establishing a regional ICT hub will only be achieved if the country also becomes a very safe place to store data, and a very safe place, where globalized and virtualized enterprises can discover the structural, regulatory and operational stability and confidence that is constantly sought to conduct virtual business by all. It is therefore imperative that the move towards a deeper regional integration, and the digitization of regional economies be accompanied by more elaborate Privacy Protection instruments comparable to, and perhaps those that distance, the European GDPR [32]. Indeed, stronger privacy protection measures are already being evaluated and proposed, as part of the "*National Data Revolution Policy,"* which is nearing it's developmental completion.

Research and Development (R&D): For the first time in 15 years, the national ICT plan has prioritized R&D, in recognition of the need, and the readiness to start shifting from being passive technology consumers - to active producers of information technology hardware, software, content, applications, and services. The plan has defined five domains where the country would like to focus upon, with the strategic intention of creating a regional competitive advantage: Internet of Things (IoT), Big Data/Data Science, Cybersecurity, Creative Industries, Mobility and Digital Lifestyle.

All 5 of the identified key domains for R&D have one great commonality: Data, as the domain driver. Indeed, since Rwanda is geographically landlocked, she will always be at a competitive disadvantage when material considerations of 'use intensity' related costs involving transportation and other conveyance related logistics are under the microscope in business analyses. However, in the matter of data conveyance, travel at the speed of light is possible, and once the communication infrastructure has been deployed, and is functioning, the geographical position of any one party and, or any transactors in concern, become less relevant - in the context of our globalized existence. Today, digital economies are growing much faster than traditional ones, and the cross-border flow of data is surpassing in value, the flow of physical goods [33]. It is against this background that Rwanda has initiated the drafting of a *National Data Revolution Policy,* which seeks to define and to formalize, just how the country will turn 'data,' into an economic and social advantage, which is only possible when the security of data and privacy of citizens is assurable and maintainable too. The *National Data Revolution Policy* will therefore be mandating what needs to be done, in complement to all current efforts that are underway, in order to properly build the human, technical and institutional capacities necessary to protect data and privacy, in addition to the implementation of the necessary legal and regulatory instruments.

5 Privacy protection and digital transformation – essential national components

The modern roots of privacy protection for the digital century in Rwanda, began with the formulation of the nation's digital transformation vision and strategy. One of the earliest shifts in this direction emerged in 1997, with the establishment of the first computer science school and programs, at the National University of Rwanda, and also to transform the country's military school and largest military barracks located in Kigali's City Centre, into a Science and Technology Institute. The initial curriculum included programs focusing on computer security as a strong component to student education, to equip the first graduates - with knowledge and the leadership ability for instance, to provide the necessary stewardship skills for Personal Privacy and information security for the digital century, and beyond. More recently, in a continuous effort to raise a home-grown talent base, the government of Rwanda partnered with Carnegie Mellon University to launch its first and only Continent of Africa campus, which offers graduate studies in Information Technology, Computer Science and Electrical Engineering related majors.

Another strategic decision was for the Rwandan Government to exit the Telecom business in 2000 and to liberalize the sector. The move was accompanied by promulgation of the law Governing Telecommunications [34], which dedicated its entire 16th Chapter to "Privacy and Data Protection." According to this law, unlawful interception communications, or accessing other people's private data, is first sanctioned by a monetary fine, and secondly, through the pain of imprisonment, for up to one year.

In 2010, the Government introduced a draft ICT bill in parliament, as the first comprehensive legal and regulatory

instrument to align and direct these increasingly converging sectors. For instance, the bill provided the strongest mechanisms yet for data protection, personal privacy and for the confidentiality of personal communications. The bill[9] [5] would make history as one of the laws that took the longest to be approved by parliament, and would finally be signed into law in June 2016. In its article 102, the Bill mandates Government licensed Telecommunications providers to protect the privacy of their customers. In article 124, the law states that "every subscriber or user's voice or data communications carried by means of an electronic communications network or services, must remain confidential to that subscriber, and, or user, for whom the voice or data is intended". The bill has other provisions related to protecting users' personal information and privacy by private and public entities while performing operations such as billing, customer registration, issuing of digital signatures, etc. The regulatory authority which has the mandate to protect the customers of electronic communications and services, has availed several avenues for initiating and escalating complaints related to the services including those complaints related specifically to privacy.[10]In case a provider is convicted of abuse, the law provides for administrative sanctions that range from monetary fines, to the loss of Government provided operating license. Meanwhile, a lawful interception legislation was put in place in 2008, to provide a framework for *"the regulation of interception of communications in the interest of national security"*. The spirit of the law proposes that national security and personal privacy should not be mutually exclusive, but quite the opposite. Indeed, personal privacy is an important foundation of national security, understood in its broad sense of having a stable, cohesive and harmonious society, and vice versa.

However, as the country has moved through the many stages of digitalization, the need to have stronger national policies, legal remedies and regulatory emphasis on jurisdictions, powers and the instruments of power to protect privacy, have become more pressing than ever. Consequently, the Smart Rwanda Master Plan's implementation is expected to define Privacy as a central concern, even as we continue to learn how best to leverage: continually evolving best practices in the world, the best available Privacy Protection institutional and infrastructural frameworks from those in the world, that have been actively engaged in making their environment and services safer for their users, and the availability of tools and techniques across the multiple domains of digital transformation.

[9] Law N°24/2016 of 18/06/2016 Governing Information and Communication Technologies, Government of The Republic of Rwanda

[10] For instance, a toll free number, and an online portal has been set up for this purpose.

5.1 From a failed state to an African trailblazer in ICT

By 2005, Rwanda's ICT developments had gained a remarkable level of attention from other nations of the Continent, as well as a growing number of international community players. In 2007, the country hosted *"Connect Africa"* Summit, in collaboration with the United Nation's International Telecommunications Union (ITU), the African Development Bank (AfDB) to invite more African countries to emulate Rwanda's experience.

Fast forward to 2013, Rwanda had gained the recognition as a *Trailblazer* in ICT development, in Africa. The Smart Africa Alliance, launched in 2017 by seven countries, has now grown to 17 countries, joined by a growing number of international private sector companies, all seeking to be part of Africa's digital transformation.

The successful implementation of the Alliance's agenda [35] is expected to accelerate the digitization of important aspects of business, government and the private lives of citizens, in a cross-border context. One flagship initiative aims at promoting indigenous culture, while *"helping African countries develop globally acceptable standards, norms and methods"* to establish, stabilize and assure - a continuity framework for societal concerns such as privacy, safety and the security of data.

One early indication of the formation of the single African digital market has been the removal of cellular telephone service related roaming charges, and the enablement of cross-border mobile financial services, among all members of the Smart Africa Alliance. In the four countries of the Northern Corridor of East Africa (Kenya, Rwanda, Uganda and South Sudan) citizens are able to use their national identification cards to travel across the region, which requires the exchange of personal information among several immigration authorities. The countries have also established frameworks that enable cooperation to fight cybercrime, terrorism and other forms of threats to national and citizen safety and security.

It is expected that other members of the Smart Africa Alliance will emulate the experiences of the Northern Corridor, and will thereby facilitate the expansion of the benefits of regional integration to a much bigger market, and that the Alliance and such integrated practices will permit for better Privacy risks containment and management, in that broader digital single market. Such expectations have already triggered action within the northern corridor partner states (Rwanda, Uganda, Kenya, South Sudan), who have established a framework for data exchange and data protection within the region. The framework is expected to provide the foundational basis for countries to cooperate, in the establishment and running of, specific measures to prevent, but also prosecute - privacy related crimes that may occur in a cross border context. Conscious of her aspirational role as Africa's tech hub, Rwanda understands that privacy needs to be a

central concern to Africa's digital transformation. And while Rwanda is prepared to spearhead the mobilization of Smart Africa partner states [36], as well as to lead the broader African Union (AU) members to adopt high standards of information security and privacy protection, there is no better way to achieve that goal than to lead by example [37]. Such is that, the SRMP endeavors to accomplish.

6 Privacy, data security and safety – a top priority

From the onset of *Vision 2020*, ICT was seen as an enabler for other sectors to achieve their strategic outcomes, in both desired quality, and quantity parameters. The successive NICI plans have laid out in details for each project, clear policies and operational objectives, requirements for human resources to execute those projects, governance, reporting and monitoring and evaluations mechanisms – often with templates provided. The outcome of mainstreaming ICT into the public sector has been an incremental process, also introducing incrementally, improvement in the quality of services provided to citizen or business; but most of the time, it was an enablement of a totally new experience that could not be achieved with the most efficient paper based process.

An example in point is with the TRACnet platform [38] which was used to help manage the national HIV/AIDS program. TRACnet used simple feature phone to report on 42 key performance indicators on monthly basis from more than 400 health centers across the country. At the beginning of the program in 2005, Internet penetration in Rwanda was less than 0.1% and phone penetration was still below 3%. In a country where most of the health centers are located in rural areas, without a highly efficient postal system, it was practically impossible to obtain timely and quality data on monthly basis, which was a critical criteria and contributing factor for scaling up the HIV/AIDS program at national level. Today, Internet penetration has reached 35%, and telephonic services penetration is above 80%. Broadband Internet penetration is expected to grow rapidly in the next few years, based on the investment that is being made to extend 4G LTE coverage to at least 95% of the country by the end of 2017. By this infrastructure alone, 95% of all Government transactions with Rwandan Citizens, and those others within the national boundary who also need Rwandan Government's services will be able to interact and acquire services by 2018, through the "Rwanda Online" Platform [24].

From TRACnet implementation in 2005 to "Rwanda Online" in 2015, the need for a strong framework for Privacy protection has been clear to all key stakeholders involved in the country's digital transformation; ranging from citizens, to service providers, and to policy makers. TRACnet contained individual records of all HIV/AIDS patients receiving treatment in the country. Public health authorities took necessary measures to ensure that the information is protected at all times. Data protection mechanisms spanned from ensuring the individual records are only available at a certain time, in paper format, and only at the point of care delivery – and all digitally transmitted information is de-identified. The data had to always be encrypted and stored in country, on verified hardware, and only accessed by secure connections.

The Government strategy to protect information having a bearing on the preservation of people's privacy have always hinged on the development of clear policies, legal, regulatory and institutional frameworks; human capacity development, investment in infrastructure, and capacities to detect, investigate, respond, and to prosecute cybercrimes.

At this point, the reader must be reminded that the right to privacy is presently enshrined in Rwanda's Constitution, which now guides the development and implementation of other legal and regulatory instruments, both current and future. Article 23 of the Rwandan Constitution [3] stipulates that, *"the privacy of a person, his or her family, home or correspondence shall not be subjected to interference in a manner inconsistent with the law; the persons honor and dignity shall be respected. A person's home is inviolable. No search or entry into a home shall be carried out without the consent of the owner, except in circumstances and in accordance with procedures determined by the law. Confidentiality of correspondence and communication shall not be waived except in circumstances and in accordance with procedures determined by the law"*. This provision is in line with a number of international covenants that Rwanda has adhered to, including the *Universal Declaration of Human Rights* [39], and the *International Covenant on Civil and Political Rights* (UN Office of the High Commissioner - Human Rights [40])– to which Rwanda acceded in 1975. In Article 38 of the Rwandan constitution of 2003, as amended in 2015 [3], clearly places personal and family privacy above the freedom of press and right to access to information in the following terms: *"Freedom of press, of expression and of access to information are recognized and guaranteed by the State. Freedom of expression and freedom of access to information shall not prejudice public order, good morals, the protection of the youth and children, the right of every citizen to honor and dignity and protection of personal and family privacy."*

The adherence of Rwanda to the aforementioned covenants however, suffered a serious blow - with the Genocide against the Tutsi of 1994. Indeed, genocide, in no-uncertain terms, represents an absolute negation of people's fundamental rights, with the right to privacy among the first - to be infringed. In the particular case of Rwanda, the use of rape and sexual violence as a weapon of genocide [41], the identification of victims through their identity cards that carried ethnic group affiliations - were extreme violations of privacy, that have not been seen anywhere else in the world at such

a large scale in modern times [42]. At the time, the psychological devastation caused by such a massive violation of personal and familial privacy, threatened to plunge survivors of the genocide into a trauma that would be irreversible. Indeed, the rebirth of Rwanda, largely seen as a failed state in 1994, had to go through the restoration of the social fabric by way of a combination of unity and reconciliation initiatives, and a home grown restorative justice system locally known as *"gacaca"*. As one of the very first major decisions taken - on the road to national reconciliation and unity involved the initiation of a prime directive by government - to scrap all national identity cards that qualified one's ethnicity and related affiliations, and to start forging a new – "inclusive" and integrated societal parameters for identity, for all Rwandans.

The prosperity that resulted from Rwanda's turnaround efforts has been described as nothing short of a miracle [22], to the credit of the RPF movement which stopped the genocide. Over the last 25 years, Rwanda was recognized as the top performer globally in the Human Development Index by the UNDP.[11] [43]. During this time, which includes all of the 22 years of post-genocide period in Rwanda, the life expectancy of Rwandans has increased by 32 years, and Rwandans stay twice as long in school. Maternal Mortality Ratio was reduced by 77% between 2000 and 2013, while child mortality under-5 years of age was reduced by more than 70% [44]. The World Economic Forum's 2015 report on the Global Gender Gap also placed Rwanda as top in Africa, and number 6 globally, attesting to the leadership's will, and ability to extend equal access, and opportunities for economic participation, education, health and survival, as well as political empowerment. An important ingredient of these, and of many other successes in socio-economic transformation areas, has been the overwhelming support from the Rwandan people for their government's policies, and the great investiture of their trust in Rwanda's public institutions. This trust rose from the painful yet, highly fruitful unity and reconciliation journey that all Rwandans had to collectively undertake, post the 1994 genocide against the Tutsi, in order to mold Rwanda the nation-state it has become today; a stable, thriving and forward looking country with pronounced prospects. Throughout this revolutionary journey, Rwandans have worked with their government, hand-in-hand, to set, and to achieve goals. While being actively engaged in Rwanda's digital transformation, governance instruments to exercise and to ensure Government's responsibility to all Citizens had to be put into place, including those that direct and institute the preservation and protection of critical societal values - such as personal privacy.

[11] United Nations Development Program

7 Conclusion

The challenges related to the protection of personal information in our digital world, and indeed, this century, are complex, and requires the aggressive and focused matching of immense will, with a fiery commitment by all who are involved, toward the stewardship and the custodianship of people's Personal Privacy, to achieve civilized society's desired Privacy oriented goals. The fast changing nature of 'technology threats' to Personal Privacy requires great adaptive flexibility and agility on the part of Government entities such as regulators and law enforcement authorities - to the sometimes highly nuanced nature and the frequency of changes represented in legal frameworks, and established practices; all of which must be deliberately directed to protect.

Societal frameworks conceived and erected to preserve and protect citizen privacy for instance, must ensure that State' pursuits to succeed in policy formulation and programs administration, process and procedure maintenance, regulatory enforcement, and any administration of restorative justice - do not compromise, or otherwise suppress, citizen safety and security. Societies must endeavor to adopt the best principles that can morally ensure citizen safety and security without any compromise in personal privacy. Among the many particularities that the leadership of the Republic of Rwanda have had to study carefully, regarding the protection of personal privacy of all individuals in Rwanda, has been to investigate, and to better characterize, the limits of ICT 'user capacities and capabilities', and the environmental risks that are consequentially introduced, in order to mitigate such risks, and to properly address potential loss considerations related to personal privacy and data protection. As Rwanda continues to embrace the many processes of digital transformation for her society, the commitment from the central government will be to continue to ensure that the use of ICT, and associated societal rewards are not realized at the expense of sacrificing people's privacy. Given Rwanda's ambition of becoming an ICT Connecting-Point for the Continent of Africa, it is important that the country leads by example for all those on the Continent of Africa, and beyond, by upholding a sustained commitment to the protection of personal privacy, and to the preservation of deeply rooted Rwandan traditions related to Privacy.

Compliance with ethical standards

Conflict of interest The author declares no conflict of interest.

Funding There is no funding source for this article.

Ethical approval This article does not contain any data, or other information from studies or experimentation, with the involvement of human or animal subjects.

References

1. Schwab K. The fourth industrial revolution. Geneva: World Economic Forum; 2015.
2. Ministry of Finance and Economic Planning. Vision 2020. Ministry of finance and economic planning, government of Rwanda, Kigali: Rwanda; 2017. http://www.minecofin.gov.rw/fileadmin/templates/documents/NDPR/Vision_2020_.pdf.
3. Government of Rwanda. Constitution of the Republic of Rwanda. Parliament of Rwanda, Government of Rwanda, Kigali:Rwanda; 2015. http://www.parliament.gov.rw/fileadmin/Bills_CD/THE_CONSTITUTION_OF_THE_REPUBLIC_OF_RWANDA_OF_2003_REVISED_IN_2015.pdf.
4. Ministry of Youth and ICT. Policies and regulations. ministry of youth and ICT, government of Rwanda, Kigali:Rwanda; 2017. http://www.myict.gov.rw/fileadmin/Documents/Policies/Rwanda_Open_Data_Policy-Draft.pdf.
5. Law N°24 GO. Relating to governing information & telecommuncations technology, *laws and orders*. Rwanda utilities regulation agency, government of Rwanda, Kigali:Rwanda; 2016. http://www.rura.rw/fileadmin/docs/Law_governing_Information_and_Communication_Technologies_Levy_on_petron__27_06_2016.pdf.
6. Law N° 13 GO. Relating to the code of criminal procedure, government of Rwanda, Kigali:Rwanda; 2004. http://www.refworld.org/docid/46c306492.html [Also, In Official Gazette of the Republic of Rwanda].
7. Habumuremyi PD. Rwanda: building a model nation state. Ouagadougou: Apidama; 2013.
8. Kagame A. Inganji Karinga ["Songs of the Drum"]. Kabgayi: Publisher Unidentied; 1943.
9. Corydon B, Ganesan V, Lundqvist M. Digital by default: a guide to transforming government. New York: McKinsey & Company; 2016.
10. Greenstein B. The Internet of Things: Intelligent, instrumented, interconnected and in real time. 2015. Retrieved from IBM Big Data and Analytics Hub: http://www.ibmbigdatahub.com/blog/internet-things-intelligent-instrumented-interconnected-and-real-time.
11. GSMA. The mobile economy. London: GSMA Intelligence; 2017.
12. Bauer H, Patel M, Veira J. The internet of things: sizing up the opportunity. New York: McKinsey & Company; 2017. http://www.mckinsey.com/industries/semiconductors/our-insights/the-internet-of-things-sizing-up-the-opportunity
13. Gallagher S. Yahoo admits it's been hacked again, and 1 billion accounts were exposed; 2017. Retrieved from Ars Technica: https://arstechnica.com/security/2016/12/yahoo-reveals-1-billion-more-accounts-exposed-and-some-code-may-have-been-stolen/.
14. Zetter K. LifeLock CEO's identity stolen 13 times. New York: Wired; 2017. https://www.wired.com/2010/05/lifelock-identity-theft/
15. PATCO vs People's United Bank. Case No:11–2031 (United States Court of Appeals, First Circuit March 7 2012); 2012.
16. Preston A. The death of privacy. London: The Guardian; 2014. https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston
17. Fisher CB, Doty MW. Decoding the ethics code: a practical guide for psychologists. Los Angeles: SAGE; 2012. [Although contextually different in subject, argumentation that "Ignorance is insufficient as defense" is adequately posed]
18. Kelley MB. Experts destroy Obama's argument that Americans must sacrifice privacy for security. New York: Business Insider; 2013. http://www.businessinsider.com/us-must-sacrifice-privacy-for-security-2013-7
19. Hein B. Tim Cook warns of dire consequences if we sacrifice privacy for security. 2015. Retrieved from Cult of Mac: http://www.cultofmac.com/312272/tim-cook-warns-consequences-sacrificing-privacy-security/.
20. Galilei G. Dialogue on the two chief systems of the world [Dialogo sopra i Due Massimi Sistemi del Mondo]. Florence: Giovanni Battista Landini; 1632. Florence: Italy from https://galileo.ou.edu/exhibits/dialogue-two-chief-systems-world.
21. Swerdlow NM. Galileo's discoveries after 400 Years," American scientist, Vol. 99, No: 3, May–June 2011. American Scientist, Vol. 99, No: 3; 2011. https://www.americanscientist.org/bookshelf/pub/galileos-discoveries-after-400-years.
22. Redmond A, Crisafulli P. Rwanda, Inc.: how a devastated nation became an economic model for the developing world. New York: Palgrave Macmillan; 2012.
23. Quiang CZ-W, Rossotto CM. Economic Impacts of ICT. In: T. W. Bank, Information and Communications for Development (p. 157). The World Bank:Washington D.C.; 2009.
24. MYICT. ICT Sector Profile 2015. Ministry of Youth and ICT, Government of Rwanda, Kigali: Rwanda; 2015.
25. Mugisha I. Two men arrested for allegedly defrauding Rwf495m from Tigo. New York: The New Times; 2014. http://www.newtimes.co.rw/section/article/2014-11-20/183244/
26. Rwanda Utilities Regulatory Agency. Regulations on SIM Card registration. Government of Rwanda, Kigali:Rwanda; 2017. http://www.rura.rw/fileadmin/docs/Board_Decisions/FINAL_SIM_CARD_REGISTRATION_REGULATIONS_03.pdf.
27. Donohue B. Weak Encryption Enables SIM Card Root Attack. The Kaspersky Lab Security News Service, Woburn: ThreatPost; 2013. https://threatpost.com/weak-encryption-enables-sim-card-root-attack/101557/
28. Jennings R. Another BYOD worry: hacking via sim-card vulnerability. New Jersey: FORBES; 2013. https://www.forbes.com/sites/netapp/2013/07/22/byod-phone-hacking-sim-card/#20ac28ea503e
29. MYICT. Smart Rwanda Master Plan 2020. Ministry of Youth and ICT, Government of Rwanda, Kigali: Rwanda; 2015.
30. World Bank. Rankings. Retrieved from doing business: measuring business regulations [IBRD/IDA]:Washington, D.C.; 2016. http://www.doingbusiness.org/rankings.
31. World Economic Forum. The global information technology report 2016. Geneva: World Economic Forum; 2016.
32. Commission, European. Regulation "on the protection of natural persons with regard to the processing of personal data and on the free movement of such data" etc., European Commission. 2016. Retrieved from Official Journal of the European Union: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.
33. Manyika J, Lund S, Bughun J, Woetzel J, Kalin S, Dhingra D. Digital globalization: the new era of global flows. New York: McKinsey Global Institute; 2016.
34. Law N° 44 GO. Relating to the governing of telecommunications, laws and orders. Rwanda utilities regulatory authority, government of Rwanda, Kigali:Rwanda; 2001. http://www.rura.rw/fileadmin/laws/TelecomLaw.pdf.
35. Smart Africa Secretariat. The smart Africa manifesto. Kigali: Rwanda; 2016. http://www.smartafrica.org/IMG/pdf/smart_africa_manifesto_2013_-_english_version.pdf.
36. AU. Assembly of the Union — Twenty-Second Ordinary Session 30–31 January 2014 Addis Ababa, Ethiopia. 2014. Transform Africa: www.smartafrica.org/IMG/pdf/9659-assembly_au_dec_490-516_xxii_e.pdf.
37. Graylish G. Africa's chance to lead the next digital revolution. New York: The New Times; 2016. http://www.newtimes.co.rw/section/article/2016-06-18/200910/
38. UNDESA. Innovation for Sustanable Development. New York: United Nations Publications; 2008.
39. United Nations. Universal declaration of human rights. New York: United Nations; 1948. http://www.un.org/en/universal-declaration-human-rights/

40. UN Office of the High Commissioner-Human Rights. UN General Assembly (GA) Resolution 2200A (XXI). "International Covenant on Civil and Political Rights". Geneva: OHCHR; 1966. www.ohchr.org/en/professionalinterest/pages/ccpr.aspx
41. Reid-Cunningham AR. Rape as a weapon of genocide. Genocide studies and prevention: Vol.3, No: 3, University of Toronto Press; 2008. http://www.utpjournals.press/doi/abs/10.3138/gsp.3.3.279.
42. DesForges A. Leave None to tell the story. New York: Human Right Watch; 1999.
43. United Nations Development Program. Human development report 2015. New York: United Nations Development Program; 2015.
44. Worley H. Rwanda's success in improving maternal health. Washington D.C.: Population Reference Bureau; 2016. http://www.prb.org/Publications/Articles/2015/rwanda-maternal-health.aspx