RESPONSIBLE DIGITAL ID //

Effects of Data Governance Policies and Practices on Human Rights

Case Studies from Argentina, Estonia, Kenya, and China

Brandie Nonnecke,
Henriette Ruhrmann &
Andreas Sampson Geroski
September 2019

CITRIS AND THE BANATAO INSTITUTE
CITRIS POLICY LAB

RESPONSIBLE // DIGITAL ID:

Effects of Data Governance Policies
and Practices on Human Rights

Case Studies from Argentina, Estonia, Kenya, and China

Brandie Nonnecke,
Henriette Ruhrmann &
Andreas Sampson Geroski

September 2019

Author Contact
nonnecke@berkeley.edu
henriette_ruhrmann@berkeley.edu
andreas.sg@berkeley.edu

CITRIS AND THE BANATAO INSTITUTE
CITRIS POLICY LAB

Executive Summary

An estimated 1 billion people lack formal identification globally, restricting their ability to meaningfully participate in the economy and society.[1] In response, national digital identity (DID) systems are rapidly being deployed by a variety of actors and institutions to provide individuals with formal means of establishing their identity (ID). While these DID systems have the potential to hold great value to individuals, lack of sound data governance policies and practices present risks to individual civil and political rights.

Through an analysis of national DID systems in Argentina, Estonia, Kenya, and China, we investigate how data governance policies and practices affect civil and political rights within the areas of data protection, political participation, and inclusion of diverse ethnic identities. We conclude with priority recommendations for national DID system data governance policies and practices that should be implemented to support civil and political rights, including:

- Legally binding privacy standards for DID data collection, use, and sharing;

- Cybersecurity standards and use of Fair Information Practice Principles (FIPPs) for data collection and use;

- Robust and inclusive mechanisms to enable public consultation, auditing, and objection to data collection and use;

- Restrictions on use of data to track political ideology and civic behavior; and

- Regulatory and technical safeguards for the collection and use of data on vulnerable and marginalized populations.

Institutions deploying DID systems should put in place an iterative and multistakeholder review process informed by these recommendations. This process will equip stakeholders to consider the human rights impacts of data governance policies and practices throughout the life cycle of the DID system. National DID systems hold great promise to support an equitable and thriving society, but only if these systems are built on human rights-driven data governance policies and practices.

Contents

Key Terms & Abbreviations

AI	Artificial Intelligence
Data Subject	An individual or entity that can be identified directly or indirectly in a digital identity system
DID	Digital Identity
DID System	Digital Identity System: We define national DID systems as state-led digitized identity management systems, which include digital identification and surveillance systems such as digital ID ards and facial recognition surveillance systems.
DNPDP	Dirección Nacional de Protección de Datos Personales (Argentina)
ECHR	European Court of Human Rights
FIPPs	Fair Information Practice Principles
GDPR	General Data Protection Regulation (European Union)
ID	Identity
ICCPR	International Covenant on Civil and Political Rights
ITU	International Telecommunications Union
Personally Identifiable Information	Any data that can be used to identify a specific individual Information
RENAPER	National Directory of the National Registry of Persons (Argentina)
SIBIOS	Federal Biometric Identification System for Security (Argentina)
SID	Sistema de Identidad Digital (Argentina)
UDHR	Universal Declaration of Human Rights
UNHCR	United Nations High Commission on Refugees
UNHRC	United Nations Human Rights Council

01 //

INTRODUCTION

01 //

INTRODUCTION

Nearly one fifth of the world's population—an estimated 1 billion people—lacks formal identification.[2] Digital identity holds great promise to ensure that every individual is recognized under the law and is able to meaningfully participate in the digital economy and society. We define national DID systems as state-led digitized identity management systems, which include digital identification and surveillance systems such as digital ID cards and facial recognition surveillance systems. These DID systems are designed and deployed by a variety of institutions and actors, and often at speeds faster than international human rights accountability mechanisms can be implemented. While the ability for DID systems to collect and share personally identifiable information between institutions—humanitarian agencies, the private sector, and the public sector—provides substantial value, it also creates great security and privacy risks. We analyze national level DID data governance policies and practices, and in particular, the degree to which different standards promote or inhibit the protection of human rights principles.

We're at a pivotal moment where we must ensure that the data governance structures of these systems support human rights principles. To contribute to this need, we focus our evaluation on the effects of data governance policies and practices on civil and political rights. Civil and political human rights, or first-generation human rights, are both the most widely accepted group of human rights principles and the most relevant to national DID systems as they limit the state's authority vis-a-vis the individual.[3] Civil and political rights are recognized in human rights frameworks at the international and regional levels, and are fundamental within many domestic legal systems.[4,5] Recognized in the International Covenant on Civil and Political Rights (ICCPR), civil rights include ensuring an individual's right to physical and mental integrity and safety; protection from discrimination; and the right to privacy, freedom of thought, and movement and political rights include ensuring procedural fairness and due process, participation in civil society and politics, and redress and legal remedy.[6] We draw upon the work at Access Now exploring the human rights impacts of national DID systems,[7] the World Bank-coordinated Principles on Identification for Sustainable Development,[8] the International Telecommunications Union (ITU) Digital Identity Roadmap Guide,[9] the World Economic Forum Elements of Good Digital Identity Report,[10] and the Omidyar Network Good ID Framework.[11,] We propose the development of globally relevant indicators for evaluating DID system data governance policies and practices, focusing specifically on impacts on the following civil and political rights: individual liberty, security of person, procedural fairness, privacy, and non-discrimination recognized in the ICCPR.[12]

02 //

METHODS

02 //

METHODS

We explore countries that have established or are in the process of implementing DID systems to develop an understanding of the consequences of data governance policies and practices for human rights. As previously stated, we define national DID systems as state-led digitized identity management systems, which include digital identification and surveillance systems such as digital ID cards and facial recognition surveillance systems. These short case studies allow for an analysis of the different contexts in which DID systems are implemented, and how this may impact the human rights of people living in that country. Given the political and technical constraints often faced by governments when implementing DID systems, these case studies explore the trade-offs governments have made between protecting privacy and security, while ensuring maximum coverage and effectiveness of DID systems.

Case Selection

National DID systems are rapidly being adopted by countries around the world. We evaluate the human rights effects of four national DID systems representing a range of political and socio-economic contexts.

Political systems and historical events will affect how a DID system is implemented and its impact within a country. We consider countries with differing forms of government in order to evaluate appropriate safeguards that will better ensure a DID system does not infringe the civil and political rights of a population. Even for countries with similar political systems, the historical, social, cultural, economic, and infrastructure attributes specific to that country will influence the consequences of DID systems on human rights.

The historical-political context of some countries may make their populations more wary of the government collecting certain types of personal data, for instance on religion, ethnicity, tribe or gender identity, while another country’s political tensions or conflicts may make DID systems problematic for suspected exploitation or suppression of marginalized groups. Government collection of data on marginalized groups may be concerning given past, or on-going, oppression. To collect accurate data on a population and to recognize their human right to self-determination, DID systems should recognize, reflect, and respect diverse needs, including languages, differing levels of literacy and numeracy, disability, and movement constraints linked to religion, age, and gender within a country.

To ensure the case studies provide a representative account of the range of countries implementing these systems, we prioritized countries that play a regional leadership role. This could be because they have the most advanced DID system in the region, they are a regional leader for digital policy, or because the country faces challenges in implementing DID systems that other countries in the region will have to consider. Additionally, public information available on specific aspects of DID data governance policies and practices for national DID systems is limited, which constrained our selection of countries to include. We outline below how each of these factors led to our selection of the following four countries: Argentina, Estonia, Kenya, and China.

Argentina

The Argentine DID system's use of facial recognition software demonstrates the challenges of using biometric data while maintaining the privacy of the population. By linking personally identifiable information to already existing databases on the population, the Argentine DID system highlights concerns about what data government officials and security services should have access to.

Estonia

Estonia's efforts to create a holistic DID system that enables users to easily engage in the country's digital economy and society and its unique e-Residency DID system provides insight into new technology strategies and indicates what other countries could be technically capable of in the future. The cybersecurity attacks the country has faced make it an interesting case study in how it protects citizens' data and maintains access to digitized government services.[13] As a member of the European Union (EU), Estonia also provides insight into the implementation of a DID system in adherence with EU human rights frameworks.

Kenya

Due to recent ethnic conflicts and ongoing debates about the status of refugees and political affiliations within the country, Kenya provides insight into how DID systems navigate the politics of distinct ethnic identities within a country, including whether a DID denotes citizenship or residency.[14] Other countries in the region and continent may look to Kenya to benchmark DID strategies and may subsequently influence how other systems are implemented across Africa. The role of civil society and of Kenya's judiciary in overseeing its national DID system, in particular its role in determining what data can be collected, provides insight into how such systems are being shaped by increasingly proactive legal systems.[15]

China

China's DID system incorporates a broad range of mass surveillance technologies—from facial recognition to online monitoring— tied to digitized ID. China holds great influence not only in Asia but increasingly around the world. Similar technology has been replicated and sold to other countries, such as Venezuela, Ecuador, and Bolivia and will heavily influence those countries' implementation of DID systems.[16] As mass surveillance of the Uighur population in China and other minorities expands, this case study provides key insights into the human rights violations of pervasive DID systems.[17]

03 //

HUMAN RIGHTS & DIGITAL ID DATA GOVERNANCE

03 //

HUMAN RIGHTS & DIGITAL ID DATA GOVERNANCE

We evaluate the data governance policies and practices of national DID systems and their effect on ICCPR rights related to individual liberty, security of person, procedural fairness, privacy and non-discrimination in the areas of data protection, political participation, and inclusion of diverse identities.[18]

DATA PROTECTION

- Judicial Process for Access
- Restrictions on Third-Party Access
- Data Sub-Steward Compliance
- Privacy Protections
- Cybersecurity and Fair Information Practices

POLITICAL PARTICIPATION

- Public Consultation
- Public Audit
- Opportunity for Objection
- Political Party Exclusion
- Tracking Civic Behavior

INCLUSION OF DIVERSE IDENTITIES

- Options for Opt-Out
- Special Care for Protected Populations
- Registering Identity
- Information on Protected Populations
- Protection Against Misidentification

3.1 | Data Protection

Data protection is paramount to ensuring individual rights enshrined in ICCPR Articles 9 and 11, right to individual liberty and security of person; Article 14, procedural fairness; and Article 17, right to privacy. We explore whether a national DID system has established a judicial process to restrict law enforcement's access to the DID system database, appropriate procedures to oversee third-party access to data; legally enforceable compliance and accountability standards for data sub-stewards; legally enforceable privacy protections for DID data, including enabling individuals to access and correct their individual data and object to its use and management; and whether the DID system has implemented appropriate strategies and safeguards to protect the DID system from data breaches.

3.1.1 | Judicial Process for Law Enforcement to Access the Digital ID System

Procedural requirements to access a DID system and its data must strike a sensitive balance between enabling interagency cooperation and minimizing the risk of misuse. For example, both in Canada and the U.S., there are many well-documented cases when governmental databases have been used to illegally surveil individuals, including cases when law enforcement officers have exploited these systems to gain confidential information on current and former romantic partners or on persons an officer found attractive.[19,20] For this reason, it is important to establish well-balanced judicial processes to regulate which law enforcement agencies have access and standards for access privileges, including whether there are requirements for a warrant.

3.1.2 | Restrictions on Third-Party Access

The personally identifiable information stored in DID systems has great market value for private companies developing business models around the commercialization of personal data. Therefore, governments administering DID systems may be tempted to grant access to records stored in the system to third parties. It is important that rigorous restrictions be put in place regulating third-party access to DID systems and data, and, if such access is permitted, standards must be established for the vetting of third-party requestors.

3.1.3 | Legally Enforceable Compliance and Accountability on Data Sub-Stewards

Third parties who have access to the DID system and its data act as sub-stewards for the personally identifiable information contained therein. For this reason, it is important that the government's accountability for data stewardship extends to the third-party data sub-stewards. In particular, it is important that clear data use and management policies are in place and that compliance with such policies is strictly enforced.

3.1.4 | Legally Enforceable Privacy Protections Specific to Digital ID

The storage and linking of personally identifiable information about individuals increases their vulnerability with respect to overall privacy and security. It is important that comprehensive privacy legislation operationalizes the right to privacy with respect to personal data and establishes legal rights for the data subject vis-a-vis the data controller to access and correct their individual data, as well as object to data use and management.

3.1.5 | Cybersecurity and Fair Information Practices

Data breaches in a DID system could expose the most confidential personally identifiable information to nefarious actors. To mitigate this risk, DID systems should implement cybersecurity standards and be built upon Fair Information Practice Principles (FIPPs) for protecting personal information, including implementing strategies of data minimization, purpose specification for all data collected, and security safeguards that are continuously monitored and updated in relation to threat assessments.[21]

3.2 | Political Participation

DID systems should enable public participation at every stage—from public consultation in the original design to establishing adequate procedures for individuals to object to the collection and use of their data. We evaluate whether a national DID system has appropriate public consultation and audit strategies, procedures that allow end-users to review and object to the use of their data, and exclusions for access and use of civic data by political parties. DID systems should ensure individuals can exercise their rights, including ICCPR Articles 14 and 16, procedural fairness and the right to legal recognition; Article 17, right to privacy; and Article 25, the right to political participation.

3.2.1 | Public Consultation

A public consultation on DID systems is a marker of both good governance and a commitment to transparency. Given the array of technical, ethical, and implementation challenges faced by governments, consultations allow experts, civil society groups, and the public more broadly to shape and determine the remit and reach of any DID system. This not only adds to the credibility of the DID system, but provides opportunity for groups and individuals to express their freedom of speech on an area of government policy that affects their fundamental freedoms and rights. Public consultation should be sought at each stage of the process from pre-design and design; rollout and implementation strategies, including evaluation of procurement tenders and bids; to continued evaluation of the DID system as it expands and changes over time.

3.2.2 | Public Audit

Public audits on both the implementation and maintenance of DID systems are essential for the public to know its rights and the limits and provisions safeguarding those rights. In the case of DID, the public's right to privacy means individuals have a right to know what and how much information is collected, how this information is used by the government and third parties, and procedures to ensure private data are safe and secure.

3.2.3 | Opportunity for Objection

Governments must establish appropriate mechanisms whereby individuals can object to—without fear of retribution or loss of access to government services—what data are collected about them, how their data are stored, and who can have access.

3.2.4 | Political Party Exclusion

Data contained in DID systems, especially voting behavior, can be extremely valuable to political parties. The data could be used to target voters, make private information on political opponents public, and to exclude or benefit certain populations or individuals. Governments must establish appropriate safeguards to restrict the exploitation of civic data by political parties.

3.2.5 | Tracking Civic Behavior

Tracking civic behavior could stifle freedom of speech, expression, and liberty. If governments knew whether and for whom, a member of society voted or whether the person is engaged in political activity, government actors could use this to target political dissidents and restrict their access to government services. DID systems should neither be used as a form of repression to curtail the rights of a population to vote or engage freely in political activity, nor be used as a way to encourage, forcibly or otherwise, the population of that country to vote for certain political parties.

3.3 | Inclusion of Diverse Ethnic Identities

In order for a DID system to maximize value for all, it must be responsive to the preferences and needs of a diverse representation of users. Barriers to access, including legal, procedural, and social, should be identified and mitigated to better ensure universal coverage and accessibility. Special precautions must be put in place to ensure data collected on individuals who may be at risk of exclusion, discrimination, or persecution are not used to infringe on individual rights, including ICCPR Articles 9 and 17, the right to individual liberty and protection against unlawful attacks; Articles 14 and 16, procedural fairness and the right to legal recognition; and Article 26, non-discrimination and equal protection of the law.

3.3.1 | Options for Opt-Out

DID systems must allow individuals to opt-out in full or to select aspects of the DID system without risk of losing their civil and political rights, including the ability to access government services and actively participate in civic life.

3.3.2 | Special Care for Marginalized and Vulnerable populations

Inclusion of politically marginalized and vulnerable populations, including racial and ethnic minorities or the socioeconomically disadvantaged, in DID systems can pose great risk, including the use of these systems to track, manipulate, or infringe upon their rights. It is imperative that DID systems establish procedures to ensure these populations are appropriately recognized, safeguards are put in place to protect data from abuse, and that they are not subject to greater scrutiny than other population groups.

3.3.3 | Registering Identity

By not allowing certain social or cultural groups to join a DID system, governments restrict these groups from fully exercising their rights to political participation, legal recognition, and non-discrimination. Legal, procedural, and social barriers to enroll in and use DID systems should be evaluated for discriminatory practices. DID systems should include representation of diverse identity groups to ensure inclusivity and representation of all.

3.3.4 | Additional Information Collected on Protected Populations

DID systems often collect additional information on protected populations—women, children, ethnic minorities, religious groups, and forcibly displaced persons—to better understand and track their needs. However, collecting additional information from protected populations can be discriminatory and a violation of their privacy. Governments must utilize the FIPPs and engage in public consultation to justify collection of additional information on protected populations, receive approval from data subjects on data collection and use, and establish safeguards to ensure additional data are not used to discriminate or infringe upon individual rights.[22]

3.3.5 | Protection Against Misidentification

Government agencies are increasingly implementing nationwide DID systems that integrate facial recognition technologies to verify identity. However, research has shown that facial recognition technologies are not equally effective at identifying individuals of different ethnic and gender identities, raising serious concerns over bias and discrimination.[23] Misidentification infringes on a number of rights, including individual liberty and security of person, procedural fairness, and the right to privacy.

04 //

CASE STUDIES

04 //

CASE STUDIES

We evaluate the data governance policies and practices of national DID systems implemented in Argentina, Estonia, Kenya, and China. Each case study provides an evaluation of the effect of data governance policies and practices on civil and political rights within the areas of data protection, political participation, and inclusion of diverse ethnic identities.

Argentina

Overview

Argentina's Sistema de Identidad Digital (SID), is an entirely state-run DID platform linked to the Argentine National Directory of the National Registry of Persons (RENAPER), which includes information about foreign nationals living in Argentina.[24] The SID is a voluntary DID system, meaning individuals can opt-out from inclusion. After being developed in conjunction with the Ministry of Modernization, the SID is now administered solely by the Ministry for the Interior, Public Works and Housing and forms part of the Argentine government's digital strategy. SID uses facial recognition software to validate users' access to public and private services with a particular focus, for the preliminary stages, on integrating the system with health and banking services in the country.[25] Originally introduced as a mechanism to prevent crime, the facial recognition system verifies the user by matching the scan to biometric data the Argentine government already has through the Federal Biometric Identification System for Security (SIBIOS) and linked to the RENAPER database. SIBIOS was developed in partnership with the government of Cuba, which provided technical support. [26] While Argentine law enforcement must request access to the RENAPER database, they are not required to do so for SIBIOS.[27]

Data Protection

The Argentine Constitution specifically gives the right to citizens to obtain any information recorded about them in private or public sources, and, if necessary, to request its deletion or amendment.[28] The law on the Protection of Personal Data (2000) prevents any entity from handing over personal data to the state unless it is justified by legitimate public interest, and individuals can request that third parties not have access to their data.[29] However, this law is undermined by clauses that allow for personal data to be transferred to the state without a person's consent if necessary for the "performance of the duties inherent in the powers of the State" and "when the communication of data takes place directly between governmental agencies to the extent of their corresponding competencies."[30] Much of the literature notes that Argentina's intelligence agencies work with little oversight and transparency, which is of particular concern given that all federal security services have access to SIBIOS.[31,32] Legislation was also passed accompanying the introduction of SID, but this was mainly to allow biometrics, including fingerprints and facial recognition, to be a legal identification method and was not specifically linked to guaranteeing privacy standards for biometric data collected.[33]

While no security breaches of SID have been reported, there are concerns about the security of SID because Argentina does not have a national strategy for data infrastructure, which has resulted in individual ministries and local governments designing their own infrastructure for protecting data. A multitude of systems makes it harder to share data and creates a greater potential for security lapses.[34] In 2013, hackers were able to download the photo IDs of registered voters, suggesting that Argentina's identity databases may be vulnerable to cybersecurity threats.[35]

A Data Protection Bill was released in 2017 for public consultation and put before Congress in 2018.[36] The SID is a voluntary system, so some may argue that Argentines will only give their data in order to access services more seamlessly; in other words, they may choose to sacrifice privacy for convenience.[37] However, individuals may feel pressure to use the system in order to ensure they can efficiently and effectively gain access to services and exercise their rights, calling into question whether the system is actually voluntary in practice.

Political Participation

Historically, the Dirección Nacional de Protección de Datos Personales (DNPDP), the national data protection agency, had a path for Argentines to object to use of their data by either public or private sources, and proposed draft legislation similar to the EU General Data Protection Regulation (GDPR), which establishes standards for data protection and privacy for all citizens of the EU.[38] However, the effectiveness of DNPDP has been questioned, given it operated with a small budget and was close to the executive branch of government.[39] Moreover, in September 2017, a new body, the Agencia de Acceso a la Información Pública, replaced the DNPDP, with this agency falling under the control of the executive branch, raising concerns about how the government may approach data protection and questioning the agency's independence.[40] The current policy states that individual requests for information on how data are being used can be done free of cost only once every 6 months, which in effect hinders Argentines' ability to discover how their data are used.[41]

Despite these concerns, no evidence has yet come to light that political parties have access to the DID system or that it tracks how Argentines vote. With reports that some populations in Argentina have their identity cards removed to prevent them from voting, the potential use of SID in voting could actually improve democratic freedoms in the country by enabling a greater number of people to vote.[42] However, concerns that the SIBIOS database is being used for purposes beyond its original intent, such as to cross-check citizens' photographs during voter registration in the 2013 and 2015 elections, have raised questions over whether adequate privacy safeguards have been instituted.[43] This shows the importance of data security in the use of DID systems, not least if it is used to register voters.

Inclusion of Diverse Ethnic Identities

SID is not mandatory and is not the only way to access public services, it just makes it easier to do so. This allows individuals to, in effect, opt-out of the DID system if they are uncomfortable with the government collecting their personally identifiable information and they do not lose their recognition before the law by doing so.[44] Because SID requires access to a mobile device and the internet, remote or rural populations may be excluded due to the inability to enroll and authenticate their enrollment online. The Argentine Data Protection Agency also specifically states that citizens are not required to disclose data about their ethnicity, thereby establishing a safeguard to better ensure the DID system is not used to target certain ethnicities within the country.[45]

Summary

While Argentina has both privacy legislation and an independent body to process data requests, the executive control over this body and the caveats allowing government access contained within this legislation undermine privacy safeguards. Of particular concern is the security services' unfettered access to the SIBIOS system, which links to Argentina's DID system. Given that this DID system relies on biometric data, a lack of protection from unwarranted state access is a worrying threat to the privacy and human rights of the Argentine population. While no specific cybersecurity vulnerabilities have yet been reported for the SID, the lack of a national digital infrastructure policy creates security and privacy vulnerabilities. In summary, the framework within which Argentina's DID system is being implemented creates cause for concern about how this could be used to infringe and violate the human rights of Argentines.

Estonia

Overview

Estonia offers one of the most comprehensive DID systems in the world. The state-issued ID card provides verified identification and access to Estonia's e-services, including voting, filing taxes, incorporating a business, accessing healthcare, and many more.[46] Estonia has established additional DID systems to facilitate the country's e-services, including Mobile ID, which provides a secure ID accessible through a mobile phone SIM card; e-Residency, a transnational DID that allows anyone in the world to become an 'e-resident' of Estonia, allowing the individual to incorporate a business or utilize e-services; and Smart ID, allowing an individual to enter a secure PIN to access financial services and digitally sign documents.

While the ID card is state-issued, the software behind the cards was developed by Estonian companies, in effect making the system a public-private partnership. The 'Smart ID' system has the highest level of EU recognition, meaning all EU member states must recognize its legality.[47] Passed in 2000, the Digital Signature Act grants equal authenticity to digital and handwritten signatures, and all authorities in the country accept digitally signed documents as legally binding.[48] Estonia's investment in its DID system has been associated with significant economic benefit and government savings and efficiencies. The Estonian government estimates that every citizen saves an average of 5 business days through the productivity gains of using the DID system, equivalent to a 2% increase in GDP.[49] As of September 2018, nearly 100% of Estonians using their digital ID, and digital signatures had been used almost 350 million times by Estonia's population of 1.3 million.[50]

Data Protection

Information on security breaches for DID systems can be hard to ascertain. For security reasons, governments have little incentive to publicize threats to the security of the system. Researchers have found this to be the case in Estonia, where evidence of significant vulnerabilities and attacks on its system have been lacking.[51] However, in 2017 a security weakness was found in the hardware behind the chips in the Estonian ID card, leading the government to suspend access to e-services for the owners of nearly 750,000 cards. The new 'Smart ID' does not require these chips.[52, 53] Estonia has taken further steps to enhance the security of its DID system by opening a 'data embassy' in Luxembourg that backs up data stored on citizens in case of a breach or cybersecurity attack on Estonia's internet or digital infrastructure.[54] Another technical security feature is the development of the 'X-Road' environment, a security layer that encrypts and tracks the data communicated between the databases and institutions, without viewing it.[55] This keeps the data secure, while also ensuring X-Road itself does not become a vulnerability.

In addition to cybersecurity safeguards, accompanying legal protections have been established to ensure data protection for Estonian citizens. In December 2018, the Estonian government passed the Personal Data Protection Act that guarantees "the right of the person to inspect his or her data and to correct, delete, or restrict his or her data and the procedure for exercising their rights."[56] This law is implemented by the Estonian Data Protection Inspectorate (hereinafter referred to as "Data Inspectorate") and includes provisions to ensure compliance with the EU GDPR.[57] Estonian citizens have the legal right to monitor how their data are stored and accessed and they own all information recorded about them. However, reports are mixed as to whether this right has been consistently respected by the government.[58,59,60]

As a member of the EU, Estonia must adhere to the European Court of Human Rights (ECHR) and European Convention on the Protection of Human Rights and Fundamental Freedoms, which recognizes the rights of minors and adults to an identity. In practical terms, this means Estonia must accurately record and protect information on an individual's identity.[61] Estonia must also comply with the ICCPR, which includes Article 1, detailing an individual's right to self-determination and is monitored by the United Nations Human Rights Council (UNHRC).[62, 63] EU members must report to the UNHRC every four years as to how they are adhering to Article 1 of the ICCPR. This is important within the context of Estonia's DID system, as it means Estonia must allow for individuals with a DID, including all Estonian citizens or migrants with a valid residency card, to not just have a right to privacy, but also to be recognized under this identity.[64,65]

Political Participation

The Data Inspectorate, operating under the Estonian Ministry of Justice, publishes annual reports to monitor, implement, and regulate data protection in Estonia. The Data Inspectorate provides opinions on draft legislation that could affect data privacy of Estonians, processes freedom-of-information requests relating to data privacy, provides information and training to businesses and residents on data privacy, and registers and licenses the use of personal data in Estonia for research or transfer of data.[66]

The Estonian DID system is also leading profound changes in the ways Estonians view and interact with their government. For instance, in the latest elections almost 30% of votes were cast electronically via the DID system. Not only did this save 11,000 working hours for government officials administering elections, but 20% of Estonians now say they wouldn't vote in a physical polling station.[67] To ensure the anonymity of voters, after the voter has been verified as eligible to vote, their vote is encrypted and can only be decrypted by the electoral commission once personal data have been removed.[68] This process is audited by the Estonian Electoral Office and is independent of any political party.

Inclusion of Diverse Ethnic Identities

Estonia's DID system, especially its e-Residency system, is inclusive of diverse identities regarding country of origin. In 2014, Estonia became the first to offer e-residency by granting anyone in the world an Estonian DID to set up a business and access public e-services.[69,70] So far, individuals from 160 countries have applied, with weekly e-Residency applications exceeding Estonia's birth rate. [71,72]

Summary

Estonia's DID system is a product of the broader technological developments pursued by the government since the turn of the century. Estonia has put in place strong technical, legal, cybersecurity, and privacy safeguards to protect data collected within its DID system, including by backing up data, establishing a security procedure to encrypt and track data when transferred between databases, and engaging in public consultation and education on data privacy. In order to actively participate in the Estonian digital economy and society, one must be enrolled in its DID system. This requirement makes enrollment essentially mandatory. Thus, it is imperative that the Estonian government continue to develop effective safeguards to ensure the security and privacy of data it holds on individuals. Its DID scheme will only be successful if users trust that their data are secure and privacy is upheld.

Kenya

Overview

In June 2018, Kenya established the National Integrated Identity Management System (NIIMS), commonly referred to as 'Huduma Namba' (Swahili for "service number"), through Executive Order No. 1 2018 by President Uhuru Kenyatta.[73,74,75] The development of NIIMS is the responsibility of the State Department for Interior, a subordinate division of the Ministry of Interior and Coordination of National Government. NIIMS expands on the capabilities of the previous Integrated Population Registration System (IPRS).[76] The National Assembly formally created the NIIMS mandate as part of the 2018 Miscellaneous Amendments Act of November 2018, signed into law in December 2018 by President Kenyatta.[77]

NIIMS seeks to consolidate identity data previously held by various government agencies into a new "master database [as] the single source of persons' identity in Kenya."[78] Problems in the former system of identity management include a lack of information flow and interoperability between government agencies, which resulted in delays in processes and vulnerability to fraud.[79] The 2017 general elections highlighted that the lack of harmonized records led to fraud on the part of candidates seeking to prove they fulfilled the "educational, moral and ethical requirements" to run for office. Some provided fraudulent documentation of their educational attainment, financial statements, and criminal records with no opportunity for verification.[80,81] NIIMS is intended to create a trusted identity by digitally capturing and storing the identity data of Kenyan citizens and registered foreign residents who will each be assigned a unique national identification number to authenticate personally identifiable information.[82]

NIIMS deployment began in several stages, including pilot deployments in 15 counties from February to March 2019 and national mass registration from April to May 2019.[83] Because of a lack of public consultation before rollout, in February 2019 the Nubian Rights Forum, the Kenya Human Rights Commission, and the Kenya National Commission on Human Rights filed a lawsuit against the federal government to stop the deployment of NIIMS due to privacy and security concerns. The resulting ruling by the High Court in April 2019 resulted in a temporary injunction on the NIIMS deployment to exclude the collection of biometric DNA data and GPS coordinates, and mandatory enrollment in NIIMS, preventing registration to be considered a condition for access to public benefits.[84] However, if the Huduma Bill introduced in July 2019 is passed registration in NIIMS will become mandatory to access government services, including obtaining a marriage certificate and accessing medical services, and steep fines will be imposed on those who do not enroll.[85,86]

Data Protection

The amended Registration of Persons Act requires that all citizens in Kenya age 18 or older provide the following information on record: (1) registration number; (2) name (in full); (3) sex; (4) county of birth or county of residence; (5) date of birth or apparent age, and place of birth; (6) occupation, profession, trade or employment; (7) place of residence and postal address, Global Positioning Systems [GPS] coordinates, Land Reference Number, Plot Number or House Number, if any; (8) biometric data, including finger and thumb impressions but in case of missing fingers and thumbs, palm or toe impressions in physical form; (9) date of registration; and (10) "such other particulars as may be prescribed."[87] These data are still collected in NIIMS. In the original rollout, "biometric" data was specified to include fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and DNA. [88] The Nubian Rights Forum, the Kenya Human Rights Commission, and the Kenya National Commission on Human Rights challenged the collection of such sensitive personal information. During the judicial process, the relevant government agencies conceded that the collection of DNA and GPS coordinates posed privacy and security risks and could not be collected.[89] The High Court affirmed the exclusion of DNA and GPS data and ordered that pending a future judicial hearing and determination, registration may not be mandatory and may not be a condition for the provision of public services or access to public facilities. The court preliminarily prohibits the sharing of data collected in NIIMS with "any other national or international government or non-governmental agencies or any person."[90] The Registration of Persons Act does not contain explicit provisions governing access to the NIIMS system for government agencies; however, according to former Permanent Secretary for the Ministry of Information and Communications, Prof. Bitange Ndemo, any agency wishing to access information contained in NIIMS needs to obtain a warrant and there are no avenues for third-party access.[91] The government restricts access of third parties such as political parties stating that “data will only be accessible by authorized officers and government agencies for official use only.”[92]

Privacy International criticizes the discrepancy between the speed of the NIIMS enactment and slow deployment of legal protections, such as the Data Protection Bill first announced in 2012 and reintroduced in July 2018 that would establish rights for individuals to access, audit, and object to the collection and management of their personal data.[93,94] At present, legal protections regarding the NIIMS system stem from the 1998 Kenya Information Communication Act, which mandates cybersecurity standards and establishes substantial fines and lengthy prison terms as a consequence of attempts to gain unauthorized access to the system.[95] However, as the Kenya Human Rights Commission highlights, the law establishing NIIMS itself does not provide specific protections for the handling of sensitive personal data, including judicial processes for accessing the system.[96] Prof. Bitange Ndemo notes that at present, data collected during NIIMS enrollment is stored on decentralized hard drives unconnected to the internet.[97]

Political Participation

Public participation is enshrined in the Kenyan Constitution as a national value and principle of governance (Art. 10 (2)(a)) and the Parliament is mandated to facilitate participation and involvement in legislative affairs (Art. 118 (1)(b)).[98] The fast-paced deployment of NIIMS began without an opportunity for the public to comment on plans for the system in a public consultation period, a gap that was sharply criticized by human rights advocates.[99] Human rights lawyer Nasanga Aki condemns the unusual legislative process of including a policy change with such wide-ranging consequences in a “Miscellaneous Amendments Act” normally reserved for minor changes to a law.[100] Moreover, the Kenya Human Rights Commission criticizes the lack of provisions on handling personal data in the law.[101] For example, the right to access, audit, and object to the management of one’s personal data by the data controller have yet to be included in the Data Protection Bill.[102] Still, political parties are excluded from accessing the system and the government dissociates the NIIMS system from voter registration: “NIIMS, census, and voter registration are completely different exercises in mandate, format, procedure or operation.”[103]

Inclusion of Diverse Ethnic Identities

The Kenyan Human Rights Commission also voiced concern that the lack of legal identification of individuals from certain ethnic minorities in NIIMS, as well as border and pastoral communities, might lead to their exclusion and effective statelessness.[104] Concerns have been raised on the inclusiveness of the NIIMS system for the Somali, Nubian, Makonde, and Shona communities because registration requires identification documents these communities have previously struggled to obtain.[105] Kenyan Somali and Nubian individuals are restricted in the days they can apply for identification documents and subject to elevated scrutiny in the process, which may, for example, include an appearance before a security panel.[106] The Somali population in Kenya includes groups whose claim to Kenyan citizenship is more or less ambiguous, including Kenyan Somalis who settled in the border regions or are rooted in colonial towns with a strong claim to Kenyan citizenship but also a large number of Somali refugees, whose status became debated when they were registered as citizens prior to elections.[107] According to Prof. Ndemo, one goal of the NIIMS enrollment process is to clarify respective claims to citizenship.[108]

To address these and other concerns, the Nubian Rights Forum filed a petition with the High Court and appeared as a petitioner in the court ruling.[109] The court's ruling excludes collection of DNA from the approved biometric data that can be collected in NIIMS due to concerns regarding ethnic discrimination.[110] Moreover, the establishment of NIIMS and the collection of biometric information raises concerns for the gay community and sex workers who have been fighting plans by the Ministry of Health to use biometrics to register members of their communities since 2016.[111]

Summary

While Kenya did not initially engage in a public consultation process before implementing NIIMS, civil society stakeholders were able to effectively use the judicial review process to establish privacy and security safeguards. The judiciary has served a significant role to ensure that NIIMS creates strategies to keep data secure and protected against exploitation; restrict third party access, including by political parties; and dissociate voting and census data from NIIMS data. Yet, additional legal oversight is needed through the Data Protection Bill, which could be used to establish legal safeguards for individuals to access, audit, and object to the collection and management of their personal data. These safeguards are especially important for ethnic minorities whose data may be used to track or restrict their access to government services.

China

Overview

China embraces emerging technologies to collect and manage identity information about its citizens in the framework of a number of large-scale government programs. Through government funding and administrative resources, China has the capacity to collate an extraordinary wealth of data on each citizen ranging from characteristics of appearance to information about activity on- and offline. To connect personal records maintained in each system, the government relies on the number associated with each citizen's digital national identification card used to access many public and private services.[112] The national ID cards issued to citizens above the age of 16 contain basic biographic information, including name, birth date, gender, address, ethnicity, and a photo.[113] Both physical and digital versions of the ID card are issued.[114] In 2017, trials in Guangzhou allowed individuals to virtually link their ID card via facial recognition to the ubiquitous messaging app WeChat owned by Tencent, indicating private sector access to at least some data stored on the ID cards.

The following brief overview introduces major programs through which the Chinese government collects data points on each individual, including physical location; biometric data, including DNA; and on- and offline surveillance of social behaviors.

Physical Movement: Skynet, Sharp Eyes, Police Cloud, and Integrated Joint Operations Platform

The Skynet Program was launched jointly by the Ministry of Public Security and Ministry of Industry and Information Technology in 2005 and completed in 2017 with the installation of 176 million CCTV surveillance cameras.[115,116] The system is on track to expand to 600 million cameras by 2020, making it the world's fastest growing government surveillance technology program in the world.[117] The program seeks to improve city management, reduce crime, and prevent disasters through installing CCTV cameras across roads, town squares, and within buildings such as hotels, malls, entertainment venues, supermarkets, hospitals, residential communities, homes of religious figures, and school campuses and classrooms.[118] In 2010, cameras started to be equipped with facial recognition capabilities.[119] In 2015, the Skynet Program was developed into the more expansive Sharp Eyes Program, inspired by the Chinese Communist Party's slogan "the people have sharp eyes," to reach the National Development and Reform Commission's goal of achieving "100% coverage" of public spaces and key industries by 2020.[120] The ambitious goal of the Sharp Eyes program's interconnectivity is to apply machine learning to the task of recognizing suspicious patterns in citizens' behavior and "predict the activities of activists, dissidents, and ethnic minorities," including those authorities say have "extreme thoughts" that pose a threat to regime stability.[121] According to Human Rights Watch, the Ministry of Public Security clearly defines seven categories of "focus personnel," including: those who "undermine stability" or "tend to cause disturbances," those involved in terrorism or drugs, major criminals and wanted persons, and those with mental illness.[122]

The Sharp Eyes Program is connected with the Police Cloud System as a backend database, an ambitious information-sharing project linking provincial police databases in a nationwide police cloud, ordered by the Ministry of Public Security in 2015.[123] In addition to connecting police forces through the network, the program has implemented pilots to facilitate the mobilization of watchful neighbors as informants by allowing them to see CCTV footage on their devices and directly report suspicious incidents to the police[124] The wealth of personal data and information linked in the system is extraordinary, including biometric and health data; travel information and monitoring of movement through CCTV footage; online information, including social media usernames, IP and MAC addresses, e-commerce transactions and purchase data.[125]

DNA: Golden Shield Project & Forensic Science DNA Database System

The collection of DNA data began in connection with the Golden Shield Project launched in 2000 by the Ministry of Public Security in an effort to build a "nationwide, intelligent digital surveillance network" with state access to personal records.[126] Since its inception, the database had developed into what the government claims to be the biggest DNA database in the world with around 54 million entries and a plan to expand the capacity to 100 million entries by 2020.[127] Police notices indicate that the accumulation of biometric information is to be used to solve crimes and the collection targets "focus personnel," i.e., individuals perceived as potentially threatening including dissidents, activists, petitioners, and anyone with a prior criminal record; "work targets," i.e., persons of interest or with criminal history; and migrants. However, evidence shows that police gather DNA samples from individuals who are not connected to or suspected of criminal activity at roadside ID checks, as well as at their homes, schools, and workplaces.[128] Moreover, individuals have been required to submit DNA samples in the course of their applications for ID documents from the police. This practice is documented but formally in conflict with Article 130 of the Criminal Procedure Law, which limits DNA collection to investigations of specific criminal cases.

On- and Offline Behavior: Cybersecurity Law & Social Credit System

President Xi Jinping has established strong oversight over the internet and the interactions of providers and consumers based on rules imposed by the national government and agencies.[129] The Cybersecurity Law, put into effect in 2017, enables the government to formalize its primacy over internet providers by requiring them to collect the real names of internet users, monitor content, and report and supply data to the national government. Enforcement of the regulations by the Cyberspace Administration of China is often strict and many companies are individually reprimanded. In 2017 alone there were over 2,000 meetings with the regulator.[130]

In 2014, China's State Council announced another nationwide DID system, the "Social Credit System," whose goal is to assess and rate the financial and social behavior on- and offline of individuals and organizations with the plan to include each citizen by 2020.[131] Most information is drawn from a collection of 400 government datasets supplied by various government agencies. The consolidated Social Credit System's database combines data from these sources and makes it searchable with biometric indicators.[132] The government has historically maintained blacklists meant to punish people who have committed infringements of the law by restricting their use of goods and services.[133] By mid-2018, blacklisted individuals had been prevented from purchasing more than 11.14 million flights and 4.25 million high-speed train tickets.[134] These blacklists are maintained by various institutions and will likely make their way into a consolidated social credit system.

Data Protection

The Chinese government has vast legal privileges to access citizens' data, including "almost unlimited and unfettered access to private sector data."-[135]Considering the sweeping access to a wealth of personal data, China has been criticized for lack of independent oversight and its justifications for broad exceptions on constitutional protections for law enforcement and protecting national security. Both China's constitution and legislation stands out in its prioritization of surveillance capabilities for the state. The National Security Law grants access to electronic communications of any organization or individual and accessing surveillance data is possible for a judicial officer without a court order.[136] However, in May 2018, the Personal Information Security Specification came into effect as a new national standard for data protection with certain provisions for private sector collection of data comparable to or further reaching than the EU's GDPR, although it is a non-binding guideline with no penalties.[137] A final version of the Guideline for Internet Personal Information Security Protection was introduced in April 2019 to protect personal data against cybercrime and a Personal Data Protection Law is expected to be introduced by the end of this year.[138,139] These developments are considered to be a result of increasing public demand for privacy protections from collection and use of data.[140] While some progress is being made to secure personal data, data collection and resale are still of serious concern. China is increasingly struggling with regulating a shadow market for personal data. For example, data bought by third parties from the department of motor vehicles or police stations is often re-sold, including to insurance firms.[141] Moreover, China experienced a large-scale breach in a facial recognition database specifically used to capture data on the Uighur Muslim population in the Xinjiang region. The database contained data on over 2.5 million data subjects, including sensitive information such as names, ID card numbers, ID card issue and expiration dates, sex, nationality, home addresses, dates of birth, photos, and employer.[142]

Political Participation

Although China engages in some processes of public consultation, these consultations are conducted primarily with elite business and political leaders.[143] The Chinese Communist Party recognizes the advantages of connecting with its citizens as a necessary means to keep policymaking flexible enough to maintain an authoritative regime. A wealth of personal information collected in surveillance systems is tied to unique identifiers within the national ID card that is specifically accessible to the Chinese Communist Party.[144] Party officials are alerted to politically relevant developments that surface in the evaluation of personal data. Through the combination of data access and alert mechanisms, the Chinese government and in particular the Chinese Communist party relies on surveillance systems to track political activities both on- and offline.

Inclusion of Diverse Ethnic Identities

Citizens have limited opportunities to opt out of data collection schemes connected to their identity information by the Chinese government. The national ID card is mandatory for all Chinese nationals. Data collection through CCTV cameras is ubiquitous and Chinese companies have limited capacity to refuse data access requests by the government. Particularly concerning is the state-led data collection on Uighur Muslims in the Xinjiang region.[145] Following deadly riots and tension between ethnic groups, the government initiated the 2014 “Strike Hard Campaign against violent activities and terrorism” and increased its public security spending in the region to over $9 billion in 2017.[146,147] The government demanded residents in the region install a mandatory app on their smartphones, giving the government full access to all files and data.[148] Additional data collected through the program include DNA and facial recognition data.[149,150] Particularly concerning is the lack of effective protection of the database used to track sensitive information on Muslim individuals in the region as demonstrated by a recent security breach.[151] Processes and systems tested in the Xinjiang region could be scaled more broadly throughout the country, resulting in a chilling effect on the most basic human rights.

Summary

The Chinese government is able to collect and track vast amounts of private information—from DNA to an individual's physical location and on- and offline economic and social behaviors. The country lacks safeguards for data protection, including robust restrictions on third-party access to data and judicial processes to restrict access to personal information collected. The Chinese government tracks political activities both on- and offline, quelling robust political participation. Without appropriate public consultation and audit strategies, individuals have limited capacity to object to data collection and use. Additionally, lack of appropriate privacy and cybersecurity safeguards places vulnerable groups at significant risk of exploitation and marginalization, as exemplified by the surveillance of the Uighurs.

05 //

RECOMMENDATIONS

05 //

RECOMMENDATIONS

To better ensure national DID systems do not infringe on civil and political rights enshrined in the ICCPR, including individual liberty, security of person, procedural fairness, privacy and non-discrimination, we provide recommendations for data governance policies and practices in the areas of data protection, political participation, and inclusion of diverse identities.

5.1 | Data Protection

Governments must put in place appropriate procedures for third-party access to data; legally enforceable compliance and accountability standards for data sub-stewards; legally enforceable privacy protections for DID data, including enabling individuals to access and correct their individual data and object to its use and management; and cybersecurity strategies and safeguards to protect the DID system from data breaches. These policies and procedures should be put in place before deployment and be routinely evaluated and updated to keep pace with technological advancements.

5.1.1 | Judicial Process for Law Enforcement to Access Digital ID Data

National DID systems must implement a robust judicial process to regulate law enforcement agency access, including restrictions on carte blanche access by establishing tiered access privileges where access is only granted for limited and purpose specific data.

5.1.2 | Restrictions on Third-Party Access

While third-party access to DID data can present great efficiency and efficacy benefits for end-users, allowing such access also presents serious security and privacy risks. Before data are shared, knowledge and consent of the data subject should be obtained. All data shared should follow data minimization and purpose specification standards, including limiting the collection and use of data by third parties to fulfill a specific purpose.

5.1.3 | Legally Enforceable Compliance and Accountability on Data Sub-Stewards

Third parties who have access to the DID system with personally identifiable information should be held accountable for the protection of that data as sub-stewards, and governments must establish accountability mechanisms to guarantee and enforce these protections.

5.1.4 | Legally Enforceable Privacy Protections Specific to Digital ID

Storing and linking personally identifiable information increases privacy and security vulnerabilities. Comprehensive privacy legislation should be established to ensure legal rights for the data subject to access and correct individual data as well as object to data use and management in the DID system.

5.1.5 | Cybersecurity and Fair Information Practices

DID systems should be built upon FIPPs to better ensure the protection of personal information, including implementation of data minimization, purpose specification for all data collected and shared, and cybersecurity safeguards that are continuously monitored and updated in relation to threat assessments.

5.2 | Political Participation

Precautions must be taken to ensure DID systems enable equitable civic engagement and safeguards are put in place to ensure data collected cannot be used to manipulate or coerce political outcomes.

5.2.1 | Public Consultation

Public consultations allow stakeholders such as technical experts, civil society groups, and the public more broadly to shape and determine the remit and reach of any DID system. Public consultation should be implemented for all DID system deployments and further developments to ensure these systems maximize benefit to society. This transparency not only adds to the credibility of DID systems, but better ensures operation in accordance with local norms and that legal frameworks keep pace with changing technological advances.

5.2.2 | Public Audit

Data subjects have a right to know what and how much information DID systems collect, how it is used by the government and third parties, and that procedures are put in place to ensure private data are secure and used responsibly. Governments must establish independent auditing mechanisms and oversight over data governance policies and practices and should provide transparent reporting on data collection, use, and cybersecurity mechanisms.

5.2.3 | Opportunity for Objection

Having a path to object to the use of personal data is an indicator of how much individual control one has over individual privacy and liberty. Data subjects must be able to object to correct, delete, or restrict how and what data are collected about them in a DID system without fear of retribution.

5.2.4 | Political Party Exclusion

The personal data contained within DID systems are extremely valuable to political parties, in both democratic and non-democratic countries. The data could be used to target voters, make private information on political opponents public, and to exclude or benefit certain populations or individuals. Instituting restrictions disallowing political parties from accessing this data, including acquiring it through third parties, safeguards the population’s right to freedom of speech, expression and privacy, irrespective of their political beliefs or civic action.

5.2.5 | Tracking Civic Behavior

Tracking civic behaviour could stifle freedom of speech, expression, and liberty. If governments know if, and for whom, a member of society voted or is engaged in political activity, they could use this to target and exclude political opponents. Governments must put in place safeguards that protect against the exploitation of DID systems for political repression or manipulation, including encrypting voting behavior and removing personally identifiable information from voting records.

5.3 | Inclusion of Diverse Identities

DID systems often contain highly sensitive personal information. For marginalized and vulnerable populations, these data make them more susceptible to exploitation, suppression, and discrimination. Balancing the benefits of collection and collation of data should be weighed against the additional risks posed for the civil and political rights of these individuals.

5.3.1 | Options for Opt-Out

In order to ensure individuals can exercise their individual liberty, security of person, and protection from discrimination, DID systems must allow individuals to opt-out without penalty of losing their right to access government services and active participation in civic life.

5.3.2 | Special Care for Marginalized and Vulnerable Populations

Inclusion of marginalized and vulnerable populations in DID systems poses great risk, including the use of these systems to track, manipulate, or infringe upon their rights. It is imperative that DID systems establish appropriate data governance policies and practices to ensure marginalized and vulnerable populations are appropriately recognized, safeguards are put in place to protect data from abuse, and that they are not subject to greater scrutiny than other population groups.

5.3.3 | Registering Identity

By not recognizing certain social or cultural groups in a DID system, governments effectively restrict these groups from fully exercising their rights to political participation, legal recognition, and non-discrimination. Legal, procedural, and social barriers to enroll in and use DID systems should be evaluated and remedies implemented to mitigate discriminatory practices.

5.3.4 | Additional Information Collected on Protected Populations

While DID systems often collect additional information on protected populations—women, children, forcibly displaced persons—to better understand and track their needs, data collection can be discriminatory and a violation of their privacy. Governments must utilize the FIPPs and engage in public consultation to justify collection of information on protected populations, receive approval from data subjects, and establish regulatory safeguards to ensure data are not used to discriminate or infringe upon civil and political rights.

5.3.5 | Protections Against Misidentification

National-level DID systems are increasingly implementing facial recognition technologies to verify identify. Misidentification through the use of DID systems infringe upon individual liberty and security of person, procedural fairness, and the right to privacy. Use of DID systems, especially facial recognition technologies that have not yet been validated to a high threshold of accuracy, should be restricted. Governments must be transparent in the use of DID systems for identification and seek public consultation on use applications.

06 //

CONCLUSION

06 //

CONCLUSION

National DID systems are rapidly being deployed globally, enabling individuals to hold formal identification that can enable them to meaningfully participate in the economy and society. While these systems hold great value, lack of sound data governance policies and practices that affect data protection, political participation, and inclusion of diverse ethnic identities pose great risk to individual civil and political rights.

Through the evaluation of DID systems in Argentina, Estonia, Kenya, and China, we have explored priority strategies for data governance policies and practices that should be implemented to support civil and political rights, including: legally binding standards for DID data collection, use, and sharing; cybersecurity standards and use of FIPPs for data collection and use; mechanisms to allow public consultation, auditing, and objection to data collection and use; restrictions on use of data to track political ideology and civic behavior; and regulatory and technical safeguards for the collection and use of data on marginalized and vulnerable populations.

Institutions deploying DID systems should put in place an iterative and multistakeholder review process informed by these recommendations. This process will equip stakeholders to consider the human rights impacts of data governance policies and practices as the system expands and changes over time. National DID systems hold great promise to support an equitable and thriving society, but only if these systems are built on human rights-driven data governance policies and practices.

ACKNOWLEDGMENTS

We would like to acknowledge with gratitude the distinguished experts who took the time to talk with us and share their knowledge and advice:

- Thea Anderson, Director, Omidyar Network
- Brett Cooper, Product Manager, Branch International
- Camille Crittenden, Executive Director, CITRIS and the Banatao Institute
- Charlotte Godart, Investigator and Trainer, Bellingcat; Former Team Leader, Human Rights Center, UC Berkeley
- Moses Karanja, Policy Associate, Omidyar Network
- Meredith Kravitz, Ecosystem Manager, ID2020
- Bitange Ndemo, Professor, University of Nairobi; Former Permanent Secretary, Ministry of Information and Communications, Government of Kenya
- Graham Webster, Fellow and Coordinating Editor, Stanford-New America DigiChina Project

Icons from Flaticon created by Smashicons, Monkik, Turkkub, and Vectors Market. All images are royalty free from Pexels.com and Pixabay.com.

REFERENCES

1. Desai, V., Diofasi, A., & Lu, J. (2018, April 25). The global identification challenge: Who are the 1 billion people without proof of identity? The World Bank. Retrieved from https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity

2. Desai, V., Diofasi, A., & Lu, J. (2018, April 25). The global identification challenge: Who are the 1 billion people without proof of identity? The World Bank. Retrieved from https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity

3. Weston, B. H. (1984). Human Rights. Human Rights Quarterly, 6(3), 257–283.

4. International Covenant on Civil and Political Rights (ICCPR). (1976, March 23). Retrieved from https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx; United Nations General Assembly. (1948). Universal Declaration of Human Rights (UDHR). Retrieved from http://www.un.org/en/universal-declaration-human-rights/

5. European Convention on Human Rights. (1953). Retrieved from https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c

6. International Covenant on Civil and Political Rights (ICCPR). (1976, March 23). Retrieved from https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx; United Nations General Assembly. (1948). Universal Declaration of Human Rights (UDHR). Retrieved from http://www.un.org/en/universal-declaration-human-rights/

7. Aggarwal, N., Ben-Hassine, W., & Chima, R. (2018 May). National digital identity programmes: What's next? Access Now. Retrieved from https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf

8. World Bank. (2017). Principles On Identification For Sustainable Development: Toward The Digital Age. World Bank. Retrieved from http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-English-ID4D-IdentificationPrinciples-Folder-web-English-ID4D-IdentificationPrinciples.pdf

9. International Telecommunications Union (ITU). (2018). Digital Identity Road Map Guide. Retrieved from https://www.itu.int/en/ITU-D/ICT-Applications/Documents/Guides/ITU_eID4D_DIGITAL%20IDENTITY_ROAD_MAP_GUIDE_FINAL_Under%20Review_Until-05-10-2018.pdf

10. World Economic Forum (WEF). (2018, Sept.). Identity in a digital world: A new chapter in the social contract. Retrieved from http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

11. Omidyar Network. (2019, May). Omidyar Network unpacks good ID. Retrieved from https://www.omidyar.com/sites/default/files/ON%20Unpacks%20Good%20ID_Final_3.7.19.pdf

12. International Covenant on Civil and Political Rights (ICCPR). (1976, March 23). Retrieved from https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

13. Sterling, B. (2018, January 09). Estonian cyber security. Wired. Retrieved from https://www.wired.com/beyond-the-beyond/2018/01/estonian-cyber-security/

14. Nyaura, J. E. (2018). Devolved Ethnicity in the Kenya: Social, Economic and Political Perspective. European Review Of Applied Sociology, 11(16), 17-26. doi:10.1515/eras-2018-0002

15. Freytas-tamura, K. D. (2017, September 01). Kenya Supreme Court Nullifies Presidential Election. The New York Times. Retrieved from https://www.nytimes.com/2017/09/01/world/africa/kenya-election-kenyatta-odinga.html

16. Berwick, A. (2018, Nov. 14). How ZTE helps Venezuela create China-style social control. Reuters. Retrieved from https://www.reuters.com/investigates/special-report/venezuela-zte/

17. Human Rights Watch (2019, March 05). UN: Act to end China's mass detentions in Xinjiang. Retrieved from https://www.hrw.org/news/2019/02/04/un-act-end-chinas-mass-detentions-xinjiang

18. International Covenant on Civil and Political Rights (ICCPR). (1976, March 23). Retrieved from https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

19. Lynch, J. (2018). Face Off: Law Enforcement Use of Face Recognition Technology. Electronic Frontier Foundation. Retrieved from https://www.eff.org/wp/law-enforcement-use-face-recognition

20. Grant, M. (2019, March 20). 3 Calgary officers who "made the police available for sale" sentenced to jail in corruption case. CBC News. Retrieved from: https://www.cbc.ca/news/canada/calgary/calgary-police-morton-mcnish-braile-sentencing-harassment-corruption-1.5064293

21. International Association of Privacy Professionals [IAPP]. (2019). Fair Information Practice Principles. Retrieved from https://iapp.org/resources/article/fair-information-practices/

22. Kaurin, D. (2019). Data Protection and Digital Agency for Refugees. Centre for International Governance Innovation. Retrieved from https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees

23. Buolamwini, J. & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of the 1st Conference on Fairness, Accountability and Transparency, in PMLR 81:77-91

24. SID - Sistema de Identidad Digital. (2019, March 19). Retrieved from https://www.argentina.gob.ar/sid-sistema-de-identidad-digital

25. Pino, M. (2018, September 03). Argentina innovates with digital identity system. Bit Finance. Retrieved from http://bitfinance.news/en/argentina-innovates-with-digital-identity-system/

26. Roveri, F., & Fascendini, F. (2014). "Your software is my biology": The mass surveillance system in Argentina. Global Information Society Watch. Retrieved from https://giswatch.org/en/country-report/communications-surveillance/argentina

27. Ferrari, V., & Schnidrig, D. (2016, October 06). State Communications Surveillance and the Protection of Fundamental Rights in Argentina. Necessary & Proportionate. Retrieved from https://necessaryandproportionate.org/country-reports/argentina

28. Constitution of the Argentine Nation, Retrieved from https://publicofficialsfinancialdisclosure.worldbank.org/sites/fdl/files/assets/law-library-files/Argentina_Constitution_1994_en.pdf

29. Roveri, F., & Fascendini, F. (2014). "Your software is my biology": The mass surveillance system in Argentina. Global Information Society Watch. Retrieved from https://giswatch.org/en/country-report/communications-surveillance/argentina

30. The Right to Privacy in Argentina (Vol. 117th, Human Rights Committee, Rep.). (2016). Asociación por los Derechos Civiles and Privacy International. doi:https://privacyinternational.org/sites/default/files/2017-12/argentina_english.pdf

31. Ibid.

32. Digital Rights LAC. (2015, May 7). Argentina: On biometrics, SIBIOS and old practices of population control. Retrieved from https://www.digitalrightslac.net/en/argentina-so-

bre-biometria-sibios-y-viejas-practicas-de-control-de-la-poblacion/

33. Ciudadanos - Una nueva tecnología al servicio de todos. (2018, November 26). Retrieved from https://www.argentina.gob.ar/sid/beneficios

34. Digital Government Review of Argentina Accelerating the digitalisation of the public sector (Rep.). (2018). OECD Digital Government and Open Data Unit. Retrieved from https://www.oecd.org/gov/digital-government/digital-government-review-argentina-key-findings-2018.pdf

35. La Nacion. (2013, November 04). Una falla de seguridad permite la descarga de fotos del padrón electoral. Retrieved from https://www.lanacion.com.ar/tecnologia/una-falla-de-seguridad-permite-la-descarga-de-fotos-del-padron-electoral-nid1635285

36. Privacy International and Asociación por los Derechos Civiles (ADC). (2019, January). State of Privacy Argentina. Retrieved from https://privacyinternational.org/state-privacy/57/state-privacy-argentina#dataprotection

37. Dergarabedian, C. (2018, July 13). Chau DNI, hola “selfie”: El Gobierno lanza un sistema de identidad digital para hacer trámites, pero expertos advierten sobre sus riesgos. iProfessional. Retrieved from https://www.iprofesional.com/notas/271448-redes-sociales-tecnologia-ciberseguridad-redes-novedades-tecnolgicas-novedades-tecnologicas-Chau-DNI-hola-selfie-el-Gobierno-lanza-un-sistema-de-identidad-digital-para-hacer-tramites-pero-expertos-advierten-sobre-sus-riesgos

38. Personal data protection. (n.d.). Retrieved April 29, 2019, from https://www.argentina.gob.ar/aaip/datospersonales

39. The Right to Privacy in Argentina (Vol. 117th, Human Rights Committee, Rep.). (2016). Asociación por los Derechos Civiles and Privacy International. doi:https://privacyinternational.org/sites/default/files/2017-12/argentina_english.pdf

40. Ibid.

41. Datos personales: Tus derechos. (2019, February 15). Retrieved from https://www.argentina.gob.ar/aaip/datospersonales/derechos

42. Wang, T. (2013). Voter Identification Requirements and Public International Law: An Examination of Africa and Latin America (pp. 1-107, Rep.). The Carter Center.

43. The Right to Privacy in Argentina (Vol. 117th, Human Rights Committee, Rep.). (2016). Asociación por los Derechos Civiles and Privacy International. Retrieved from https://privacyinternational.org/sites/default/files/2017-12/argentina_english.pdf

44. Ciudadanos - Una nueva tecnología al servicio de todos. (2018, November 26). Retrieved from https://www.argentina.gob.ar/sid/beneficios

45. Argentina Data Protection Agency Posts Draft of New Data Protection Act. (2018, February 14). Retrieved from https://lavca.org/2018/02/08/argentina-data-protection-agency-drafts-new-protection-act/

46. ID-card - e-Estonia. (n.d.). Retrieved from https://e-estonia.com/solutions/e-identity/id-card/

47. Ibid.

48. Martin, A., & Martinovic, I. (2016). Security and Privacy Impacts of a Unique Personal Identifier (Vol. 4, Working Paper, Tech. No. 4). University of Oxford. Retrieved from https://www.politics.ox.ac.uk/materials/publications/14987/workingpaperno4martinmartinovic.pdf

49. Lindsey, N. (2019, April 06). The Case For and Against Digital ID. CPO Magazine. Retrieved, from https://www.cpomagazine.com/data-privacy/the-case-for-and-against-digital-id/

50. Kattel, R. & Mergel, I. (2018). Estonia’s digital transformation: Mission mystique and the hiding hand. UCL Institute for Innovation and Public Purpose Working Paper Series (IIPP WP 2018-09). Retrieved from https://www.ucl.ac.uk/bartlett/public-purpose/wp2018-

09

51. Martin, A., & Martinovic, I. (2016). Security and Privacy Impacts of a Unique Personal Identifier (Vol. 4, Working Paper, Tech. No. 4). University of Oxford. Retrieved from https://www.politics.ox.ac.uk/materials/publications/14987/workingpaperno4martinmartinovic.pdf

52. Aasmae, K. (2017, November 13). Estonia's ID card crisis: How e-state's poster child got into and out of trouble. ZDNet. Retrieved from https://www.zdnet.com/article/estonias-id-card-scrisis-how-e-states-poster-child-got-into-and-out-of-trouble/

53. Reuters (2018, Sept. 27). Estonia sues Gemalto for 152 mln euros over ID card flaws. Reuters. Retrieved from https://www.reuters.com/article/estonia-gemalto/estonia-sues-gemalto-for-152-mln-euros-over-id-card-flaws-idUSL8N1WD5JZ

54. Heller, N. (2018, May 31). Estonia, the Digital Republic. The New Yorker. Retrieved from https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic

55. Segovia Domingo, A. I., & Martin Enriquez, A. (n.d.). Digital Identity: The current state of affairs (Tech. No. 18/01). BBVA Research. Retrieved from https://www.bbvaresearch.com/wp-content/uploads/2018/02/Digital-Identity_the-current-state-of-affairs.pdf

56. Nestor, E. (2018). Personal Data Protection Act (Vol. 367, RT I, 04.01.2019, 11) (Estonia, Parliament).

57. Ibid.

58. Heller, N. (2018, May 31). Estonia, the Digital Republic. The New Yorker. Retrieved from https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic

59. Andmekaitse Inspektsioon. (n.d.). Retrieved from https://www.aki.ee/en/inspectorate/annual-reports

60. Khatchatourov, A., Laurent, M., & Levallois-Barth, C. (2015). Privacy in Digital Identity Systems: Models, Assessment, and User Adoption. Lecture Notes in Computer Science Electronic Government, 273-290. doi:10.1007/978-3-319-22479-4_21

61. Sullivan, C. (2018). Digital identity – From emergent legal concept to new reality. Computer Law & Security Review, 34(4), 723-731. doi:10.1016/j.clsr.2018.05.015

62. Ibid.

63. International Covenant on Civil and Political Rights. (n.d.). Retrieved from https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

64. Republic of Estonia Information System Authority. (2019, February 22). What is Digi-ID? Retrieved from https://www.id.ee/index.php?id=34410

65. Sullivan, C. (2018). Digital identity – From emergent legal concept to new reality. Computer Law & Security Review, 34(4), 723-731. doi:10.1016/j.clsr.2018.05.015

66. Estonian Data Protection Inspectorate. (2019, April 15). Statistics. Retrieved from https://www.aki.ee/en/inspectorate/statistics

67. White, O., Madgavkar, A., Manyika, J., Mahajan, D., Bughin, J., McCarthy, M., & Sperling, O. (April 2019). Digital Identification: A key to inclusive growth. McKinsey Digital. Retrieved from https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-identification-a-key-to-inclusive-growth

68. Estonia, State Electoral Office of Estonia. (2017, June 20). General Framework of Electronic Voting and Implementation Thereof at National Elections in Estonia. Retrieved from https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf

69. ID-card - e-Estonia. (n.d.). Retrieved from https://e-estonia.com/solutions/e-identity/id-card/

70. Benmayor, G. (2018, October 24). Who gets a 'digital identity' in Estonia? Retrieved from http://www.hurriyetdailynews.com/opinion/gila-benmayor/who-gets-a-digital-iden-

tity-in-estonia-138206

71. ID-card - e-Estonia. (n.d.). Retrieved from https://e-estonia.com/solutions/e-identity/id-card/

72. Heller, N. (2018, May 31). Estonia, the Digital Republic. The New Yorker. Retrieved from https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic

73. Capital News. (2019, February 18). Launch of pilot biometric registration kicks off in Nyandarua. Retrieved from https://www.capitalfm.co.ke/news/2019/02/launch-of-pilot-biometric-registration-kicks-off-in-nyandarua/

74. Kenya National Government Communication Centre. (2019). Brochure National Integrated Identity Management System (NIIMS). Kenya National Government Communication Centre. Retrieved from https://www.hudumanamba.go.ke/wp-content/uploads/2019/03/NIIMS-BROCHURE-suggested-edits.pdf

75. Kenyatta, U. (2018). Organization of the Government of the Republic of Kenya. Presidency. Retrieved from http://www.kilimo.go.ke/wp-content/uploads/2018/06/Executive-Order-No-1-June-2018.pdf

76. Kenya National Government Communication Centre. (2019). Brochure National Integrated Identity Management System (NIIMS). Kenya National Government Communication Centre. Retrieved from https://www.hudumanamba.go.ke/wp-content/uploads/2019/03/NIIMS-BROCHURE-suggested-edits.pdf

77. Consolidated Petitions No. 56, 58 & 59 of 2019 (High Court of Kenya at Nairobi April 1, 2019). Retrieved from https://s3-eu-west-1.amazonaws.com/s3.sourceafrica.net/documents/119025/High-Court-Ruling-on-the-Rolling-Out-of-the.pdf

78. Kenya National Government Communication Centre. (2019). Brochure National Integrated Identity Management System (NIIMS). Kenya National Government Communication Centre. Retrieved from https://www.hudumanamba.go.ke/wp-content/uploads/2019/03/NIIMS-BROCHURE-suggested-edits.pdf

79. Ibid.

80. Constitution of Kenya.

81. Ndemo, B. (2019, May 10). Interview by H. Ruhrmann.

82. Kenya National Government Communication Centre. (2019). Brochure National Integrated Identity Management System (NIIMS). Kenya National Government Communication Centre. Retrieved from https://www.hudumanamba.go.ke/wp-content/uploads/2019/03/NIIMS-BROCHURE-suggested-edits.pdf

83. Dahir, A. L. (2019, February 21). Kenya's plan to store its citizens' DNA is facing massive resistance. Retrieved from https://qz.com/africa/1555938/kenya-biometric-data-id-not-with-mastercard-but-faces-opposition/

84. Consolidated Petitions No. 56, 58 & 59 of 2019 (High Court of Kenya at Nairobi April 1, 2019). Retrieved from https://s3-eu-west-1.amazonaws.com/s3.sourceafrica.net/documents/119025/High-Court-Ruling-on-the-Rolling-Out-of-the.pdf

85. Mwangi, W. (2019, July 18). New law to make Huduma Namba compulsory. Daily Nation. Retrieved from https://www.nation.co.ke/news/New-law-to-make-Huduma-Namba-compulsory/1056-5200282-g97pkoz/

86. Government of Kenya. (2019, July 12). The Huduma Bill, 2019: Arrangement of Clauses. Retrieved from http://www.ict.go.ke/wp-content/uploads/2019/07/12-07-2019-The-Huduma-Bill-2019-2.pdf

87. Registration of Persons Act, Laws of Kenya § Chapter 107. Retrieved from http://kenyalaw.org/lex/rest/db/kenyalex/Kenya/Legislation/English/Acts%20and%20Regulations/R/Registration%20of%20Persons%20Act%20Cap.%20107%20-%20No.%2033%20of%201947/docs/RegistrationofPersonsAct33of1947.pdf

88. Ibid.

89. Consolidated Petitions No. 56, 58 & 59 of 2019 (High Court of Kenya at Nairobi April 1, 2019). Retrieved from https://s3-eu-west-1.amazonaws.com/s3.sourceafrica.net/documents/119025/High-Court-Ruling-on-the-Rolling-Out-of-the.pdf

90. Consolidated Petitions No. 56, 58 & 59 of 2019 (High Court of Kenya at Nairobi April 1, 2019). Retrieved from https://s3-eu-west-1.amazonaws.com/s3.sourceafrica.net/documents/119025/High-Court-Ruling-on-the-Rolling-Out-of-the.pdf

91. Ndemo, B. (2019, May 10). Interview by H. Ruhrmann.

92. Kenya Ministry of Interior & Coordination for National Government. (2018). FAQs. Retrieved from https://www.hudumanamba.go.ke/faqs/

93. Kenya Data Protection Bill, 2012, Retrieved from http://constitutionnet.org/sites/default/files/the_data_protection_bill_2012_revised_10th_jan2012.pdf

94. Kenya Data Protection Bill, 2018. Retrieved from http://www.ict.go.ke/wp-content/uploads/2016/04/Kenya-Data-Protection-Bill-2018-14-08-2018.pdf

95. Kenya Law Reform Commission. (2019, April 3). The Bliss of NIIMS Paradise: The Legal Context for the Huduma Namba. Retrieved from http://www.klrc.go.ke/index.php/klrc-blog/645-the-bliss-of-niims-paradise-the-legal-context-for-the-huduma-namba

96. Venkov, J. (2019, March 18). A single source of truth - Can the Huduma Namba succeed as an integrated identity management system in Kenya? Retrieved from https://www.thetornidentity.org/2019/03/18/huduma-namba-kenya/

97. Ndemo, B. (2019, May 10). Interview by H. Ruhrmann.

98. Constitution of Kenya. Retrieved from http://www.kenyalaw.org/lex/actview.xql?actid=-Const2010

99. Mahmoud, M. (2019, February 26). Case Filed to Stop New Digital ID Register in Kenya. NAMATI. Retrieved from https://namati.org/news/case-filed-stop-new-digital-id-system-kenya/

100. Dahir, A. L. (2019, February 21). Kenya's plan to store its citizens' DNA is facing massive resistance. Quartz Africa. Retrieved from https://qz.com/africa/1555938/kenya-biometric-data-id-not-with-mastercard-but-faces-opposition/

101. Venkov, J. (2019, March 18). A single source of truth - Can the Huduma Namba succeed as an integrated identity management system in Kenya?. Retrieved from https://www.thetornidentity.org/2019/03/18/huduma-namba-kenya/

102. Kenya Data Protection Bill, 2018. Retrieved from http://www.ict.go.ke/wp-content/uploads/2016/04/Kenya-Data-Protection-Bill-2018-14-08-2018.pdf

103. Kenya Ministry of Interior & Coordination for National Government. (2018). FAQs. Retrieved, from https://www.hudumanamba.go.ke/faqs/

104. Dahir, A. L. (2019, February 21). Kenya's plan to store its citizens' DNA is facing massive resistance. Quartz Africa. Retrieved from https://qz.com/africa/1555938/kenya-biometric-data-id-not-with-mastercard-but-faces-opposition/

105. Ibid.

106. Mahmoud, M. (2019, February 26). Case Filed to Stop New Digital ID Register in Kenya. NAMATI. Retrieved from https://namati.org/news/case-filed-stop-new-digital-id-system-kenya/

107. Scharrer, T. (2018). "Ambiguous citizens": Kenyan Somalis and the question of belonging. Journal of Eastern African Studies, 12(3), 494–513.

108. Ndemo, B. (2019, May 10). Interview by H. Ruhrmann.

109. Mahmoud, M. (2019, February 26). Case Filed to Stop New Digital ID Register in Kenya. NAMATI. Retrieved from https://namati.org/news/case-filed-stop-new-digital-id-system-kenya/

110. Munyua, A. (2019, February 8). Kenya Government mandates DNA-linked national ID, without data protection law. Mozilla Open Policy & Advocacy. Retrieved from https://blog.mozilla.org/netpolicy/2019/02/08/kenya-government-mandates-dna-linked-national-id-without-data-protection-law/

111. Gathura, G. (n.d.). Proposed Huduma Namba a big disappointment for gays, sex workers. The Standard. Retrieved from https://www.standardmedia.co.ke/article/2001310477/proposed-huduma-namba-a-big-disappointment-for-gays-sex-workers

112. Human Rights Watch. (2018, February 26). China: Big Data Fuels Crackdown in Minority Region. Retrieved from https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region

113. Jezard, A. (2018, April 24). China is putting ID cards on smartphones. World Economic Forum. Retrieved from https://www.weforum.org/agenda/2018/04/china-is-putting-id-cards-on-smartphones/

114. Wildau, G. (2017, December 27). China unveils digital ID card linked to Tencent's WeChat. Financial Times. Retrieved from https://www.ft.com/content/3e1f00e2-eac8-11e7-bd17-521324c81e23; Tao, L. (2018, January 23).

115. Zihan, Z. (2012, October 10). Beijing's guardian angels? Global Times. Retrieved from http://www.globaltimes.cn/content/737491.shtml

116. Qiang, X. (2019). The Road to Digital Unfreedom: President Xi's Surveillance State. Journal of Democracy, 30(1), 53–67.

117. Big Brother Watch. (2018). Face Off - The lawless growth of facial recognition in UK policing. Retrieved from https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf

118. China Public Video Surveillance Guide: From Skynet to Sharp Eyes. Retrieved from https://ipvm.com/reports/sharpeyes; Human Rights Watch. (2018, February 26).

119. Qiang, X. (2019). The Road to Digital Unfreedom: President Xi's Surveillance State. Journal of Democracy, 30(1), 53–67.

120. Rollet, C. (2018, June 14). China Public Video Surveillance Guide: From Skynet to Sharp Eyes. IPVM. Retrieved from https://ipvm.com/reports/sharpeyes

121. Human Rights Watch. (2017, November 19). China: Police "Big Data" Systems Violate Privacy, Target Dissent. Retrieved from https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent

122. Ibid.

123. Denyer, S. (2018, January 7). China bets on facial recognition in big drive for total surveillance. The Washington Post. Retrieved from https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/

124. Ibid.

125. Human Rights Watch. (2017, November 19). China: Police "Big Data" Systems Violate Privacy, Target Dissent. Retrieved from https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent

126. Wang, M. (2017, August 18). China's Dystopian Push to Revolutionize Surveillance. Human Rights Watch. Retrieved from https://www.hrw.org/news/2017/08/18/chinas-dystopian-push-revolutionize-surveillance

127. Human Rights Watch. (2017, May 15). China: Police DNA Database Threatens Privacy. Retrieved from https://www.hrw.org/news/2017/05/15/china-police-dna-database-threatens-privacy

128. Ibid.

129. Qiang, X. (2019). The Road to Digital Unfreedom: President Xi's Surveillance State. Jour-

nal of Democracy, 30(1), 53–67.

130. Ibid.

131. Marr, B. (2019, Jan. 21). Chinese Social Credit Score: Utopian Big Data Bliss or Black Mirror on Steriods? Forbes. Retrieved from https://www.forbes.com/sites/bernard-marr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/#282e76fc48b8

132. Qiang, X. (2019). The Road to Digital Unfreedom: President Xi's Surveillance State. Journal of Democracy, 30(1), 53–67.

133. Ahmed, S. (2019, May 1). The messy truth about social credit. Logic Magazine. Retrieved from https://logicmag.io/china/the-messy-truth-about-social-credit/

134. Xuanzun, L. (2018, May 20). Social credit system must bankrupt discredited people: former official. Global Times. Retrieved from http://www.globaltimes.cn/content/1103262.shtml

135. Cate, F. H., & Dempsey, J. X. (2017). Bulk collection systematic government access to private-sector data. New York: Oxford University Press.

136. Rubinstein, I. S., Nojeim, G. T., & Lee, R. D. (2014). Systematic government access to personal data: a comparative analysis. International Data Privacy Law, 4(2), 96–119.

137. Sacks, S. (2018, January 29). New China Data Privacy Standard Looks More Far-Reaching than GDPR. Center for Strategic & International Studies (CSIS). Retrieved from https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr

138. Luo, Y., Yu, Z., & Shephard, N. (2019, April 22). China's ministry of public security issues new personal information protection guidelines. Covington & Burling LLP. Retrieved from https://www.insideprivacy.com/data-security/chinas-ministry-of-public-security-issues-new-personal-information-protection-guideline/

139. Zhang, G. & Yin, K. (2019, Feb. 26). More updates on the Chinese data protection regime in 2019. International Association of Privacy Professionals. Retrieved from https://iapp.org/news/a/more-positive-progress-on-chinese-data-protection-regime-in-2019/

140. Xiaomeng, L., Manyi, L., Sacks, S. (2018, April 25). What the Facebook scandal means in a land without Facebook: A look at China's burgeoning data protection regime. Center for Strategic & International Studies (CSIS). Retrieved from https://www.csis.org/analysis/what-facebook-scandal-means-land-without-facebook-look-chinas-burgeoning-data-protection

141. Tham, E. (2018, August 23). Data dump: China sees surge in personal information up for sale. Reuters. Retrieved from https://www.reuters.com/article/us-china-dataprivacy-idUSKCN1L80IW

142. Cimpanu, C. (2019, February 14). Chinese company leaves Muslim-tracking facial recognition database exposed online. ZDNet. Retrieved from https://www.zdnet.com/article/chinese-company-leaves-muslim-tracking-facial-recognition-database-exposed-online/

143. He, B., & Thøgersen, S. (2010). Giving the People a Voice? Experiments with consultative authoritarian institutions in China. Journal of Contemporary China, 19(66), 675–692.

144. Human Rights Watch. (2018, Feb. 26). China: Big data fuels crackdown in minority region. Retrieved from https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region#

145. Kania, E. Seeking a Panacea: the Party-State's Plans for Artificial Intelligence (Part 2). Center for Advanced China Research (2017). Retrieved from https://www.ccpwatch.org/single-post/2017/11/15/Seeking-a-Panacea-the-Party-State%E2%80%99s-Plans-for-Artificial-Intelligence-Part-2.

146. Human Rights Watch. (2018, Feb. 26). China: Big data fuels crackdown in minority region. Retrieved from https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region#

147. Lucas, L. & Feng, E. (2018, July 19). Inside China's surveillance state. Financial Times. Retrieved from https://www.ft.com/content/2182eebe-8a17-11e8-bf9e-8771d5404543

148. Cook, S. (2018, April 30). China's ever- expanding surveillance state. Freedom House. Retrieved from https://freedomhouse.org/blog/china-s-ever-expanding-surveillance-state

149. Qiang, X. (2019). The Road to Digital Unfreedom: President Xi's Surveillance State. Journal of Democracy 30, 53–67.

150. Larson, C. (2018, Feb. 9). China's AI imperative. Science 359, 628–630.

151. Cimpanu, C. (2019, February 14). Chinese company leaves Muslim-tracking facial recognition database exposed online. ZDNet, Retrieved from https://www.zdnet.com/article/chinese-company-leaves-muslim-tracking-facial-recognition-database-exposed-online/

About the CITRIS Policy Lab

The CITRIS Policy Lab is a sub-organization of the Center for Information Technology Research in the Interest of Society and the Banatao Institute (CITRIS), headquartered on the UC Berkeley campus. Founded in 2001, CITRIS leverages expertise on the campuses of UC Berkeley, UC Davis, UC Merced, and UC Santa Cruz to develop technology applications with societal and economic benefits. The CITRIS Policy Lab was established in 2018 to support interdisciplinary technology policy research analyzing technology capabilities and their implications for society. Through its collaboration with public and private sector stakeholders, the CITRIS Policy Lab addresses core questions regarding the role of formal and informal regulation in promoting innovation and amplifying its positive effects on society.