Towards a
2024 PHILIPPINE DECLARATION ON INTERNET RIGHTS AND PRINCIPLES

ver 2.1.5 / 5 June 2024

DRAFT FOR COMMENTS

EXPLANATORY NOTE: BACKGROUND AND RATIONALE

On November 4th 2015, the **Philippine Declaration on Internet Rights and Principles** was formally launched after several months of collective drafting and broad consultations with civil society organizations, internet rights groups, the ICT policy community, and other public and private stakeholders. Launched at the RightsCon Southeast Asia conference in Manila in March of 2015, it was inspired by many similar global and country initiatives to evolve a vision of the internet--then already a site of much contestation--that align with shared values and principles, ever cognizant of the impact on rights and responsibilities of citizens and communities. A diverse but compact team developed the content of the first Declaration ("PhilDec1.0"), with regional consultations held in Metro Manila, Visayas, and Mindanao until from April to October 2015 to collect inputs face-to-face, as well as online, consultations.

The Declaration, initially signed by 23 organizations, was a reflection of the dreams, hopes, and aspirations of Filipinos of what the Philippine Internet should be and worth fighting for ("Isang Internet na Ipaglalaban"), circa 2015. It hoped to serve as a basis for necessary public education, policy advocacy, intersectoral networking, and broad constituency-building--on the intersection of ICTs and the internet, human rights, development, and social justice.

Contextually, PhilDec1.0 emerged at a time when social media was exploding, and many technological advances were coming to the fore. Global and national economies were undergoing unprecedented shifts driven by innovations in technology, influencing macro- and micro-economics, and impacting people's lives--from the small set of billionaires owning and running the Big Tech companies, to the typically poor local user in countless communities trying to navigate e-wallets, payment portals, and digital currencies, while the rest of us adjusting to what seemed like inevitably digitized societies and lifestyles.

Significantly, the Declaration came barely two years after the Edward Snowden revelations of State digital surveillance, and three years before the Facebook/Cambridge Analytica scandal involving private sector intrusions into our digital data was exposed. Wars and conflicts in the real world--but many waged online as well, and almost always involving cutting-edge technological applications and digital platforms--were also upon us. Harmful content was beginning to proliferate in the very platforms we use everyday, with problematic disinformation and harmful content--regularly deployed in conjunction with the ever-developing technologies--poisoning the public sphere up to this day.

Then in 2020 we found ourselves amidst a global pandemic which tested our societal systems (digital or otherwise) and accelerated what became an almost-obligatory "digital migration/transformation"--which various groups (depending on their experiences and analytical frames) either feared, welcomed, or variously criticized. For many nation states including the Philippines, the pandemic's "everything-from-home" quarantine also served as a mirror, forcing us to look at what "digital transformation" was in real life--with all of its potentials and its perils.

Significantly underpinning this past decade is how truly revolutionary were the technical advancements that have emerged--with largely unforeseen socio-technical impacts and implications (up to this age's Pandora's Box: artificial intelligence" (A.I.), in continuing trends also observed in previous technological breakthroughs).

Thus, the dawn of 2024 has brought forth a significantly altered landscape of the internet as we know it in just under a decade.

The updated **PH 2024 Declaration on Internet Rights and Principles (PhilDec 2.0)** takes into consideration such developments that impact Philippine democracy and digital rights, including the underlying *technological advancements* (e.g., developments in the digital economy including the gig economy and the role of cryptocurrencies; big data and IoT, adaptive artificial intelligence/A.I.); *socio-technical realities* (pervasive dominance of big tech platforms, and post-pandemic digital ecosystems, digitally-enabled disinformation); and other such realities. Particular attention to the significance of *human rights, gender, and environmental sustainability* underpins this effort.

This is the context of, and the rationale for, PhilDec2.0. As we struggle to monitor, interpret, engage, and influence these ground-breaking developments, we are forced to reconsider--review and reflect on, revise and renew--the premises, promises, and paradigms of our earlier Declaration, and its societal context.

We thus embark on a process similar to the previous one--with evidence- and expert-driven research to come up with a working draft--and an iterative consultative process envisioned to extend into the second half of 2024. So the March 2024 "launch" is really of a CONSULTATIVE DRAFT as it is of a CONSULTATIVE PROCESS, by which stakeholders may contribute. And when a consensus document is forged, to eventually engender an ENDORSEMENT PROCEDURE on the (semi) final outputs woven out of the iterative process.

Appropriately, it is on the 30th anniversary of the Philippine Internet this year that we embark on this exciting process today. And it is with the same spirit of critical inquiry, deliberative democracy, and consultative (e)participation, we present the **initial draft** of what will be the **2024 Philippine Declaration on Internet Rights and Principles (PhilDec 2024)**.

###

ISANG INTERNET
NA IPAGLALABAN

The 2024 Philippine Declaration on Internet Rights and Principles

DRAFT 2.1.5 (5 June 2024)

Preamble

Recalling that the Philippines is (or aspires to be) a sovereign state in South East Asia and within the global community; an archipelago with a diverse population emerging out of different histories, cultures, traditions, and languages; which profess different beliefs and ideologies, within a polity with shared democratic values;

Recognizing the spirit and letter of the 1987 Philippine Constitution in asserting that the State should value the dignity of each and every human person, shall promote social justice in all phases of national development, and protect the right of information and communication, within a framework of freedom and democracy;

Recognizing that the Internet--the global network of interconnected computers and networks, including its infrastructure, protocols, standards, and applications--plays an important role in the lives of the Filipinos wherever they may be, affecting their social, political, cultural, and economic development;

Recognizing that the Internet is and must be a global commons and also a global public good, meant to be a public resource which no one--and everyone--ultimately owns; and must primarily serve to further the broadest public interest;

Recognizing that the Internet, at its best, also promotes individual autonomy, agency, voice, and self-actualization--particularly of minorities and historically disadvantaged populations, and its open access and strategic use must be ensured for all;

Asserting that governance of the Internet should be inclusive, democratic, and rights-based, encouraging the widest possible participation of citizens and communities, particularly from marginalized and vulnerable sectors, using all possible channels of discourse and discussion, in respectful deliberation;

Noting that while the Internet has provided a platform and ecosystem for the promotion of rights and increased democratization within and beyond the country, it has nevertheless also been misused and abused, which results in a widening of pre-existing and emergent social divides, increased oppression of peoples, additional stresses to the natural environment exacerbating the climate crisis, and causing negative impacts to social capital and personal wellness;

Affirming that all human rights that apply or are enjoyed offline--particularly those enshrined in the instruments such as Universal Declaration of Human Rights (UDHR), including the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR); and that various sectoral charters such as the Convention on the Rights of the Child (CRC), Convention on the Rights of Persons with Disabilities (CRPD), and Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), and similar international documents--should likewise also apply and be protected *online*;

Emphasizing therefore the primary responsibility of the State to always respect, protect and fulfill human rights offline *and* online, in a transparent and verifiable manner, and refraining from using the Internet and its resources to curtail freedoms, diminish rights, and foment conflict;

Emphasizing also the responsibility of the private sector--especially Internet intermediaries and platforms--to respect the human rights of their users consistent with the United Nations Guiding Principles on Business and Human Rights;

We declare the following to be part of the Internet we want, the Internet we will fight for:

1. Digital Inclusion: Internet Access and Meaningful Use for All

Everyone has the right to affordable and quality access to the Internet, one still denied to almost half of the world's populations, including within the Philippines. Beyond just token connectivity (usually just to a limited number of dominant platforms and sites), the Internet must be a *gateway for all to the entire universe of publicly available content, without discrimination*. The State must take primary responsibility in narrowing various aspects of still-existing digital divides, and provide *meaningful universal access* to an *available*, *affordable* and (for the differently-abled) *accessible* Internet, ensuring an enabling environment for *fair competition* benefiting all stakeholders, free from exploitative monopoly behavior, and ensuring adequate consumer protection for everyone's *meaningful use*.

In the Philippines, an outdated and discriminatory licensing and franchise system must shift to more open access models for data and its transmission to ensure greater choice and better service for all. And consistent with the distributed nature of the Internet, and supporting the entry of more and smaller internet providers, *community-owned and community-driven information infrastructures and networks* should also be promoted as alternatives or complements to national- and international-level infrastructure.

2. Protecting and Democratizing the Architecture of the Internet

Consistent with its function as an *open, collaborative, and interoperable digital space*, the Internet's architecture, communication systems, protocols, and data formats shall be based on broadly accepted *open standards* that ensure complete *interoperability, inclusion, and equal opportunity* for all. Recognizing its fundamental distributed, decentralized, and diverse nature, everyone shall have universal and open access to the Internet and its content--free from discriminatory prioritization, filtering, or control for political or commercial purposes (i.e., "net neutrality")--while allowing for legitimate technical traffic management and secure operations.

The Internet should continue to evolve via open, permission-less innovation and the voluntary adoption of technical and non-technical standards through inclusive multi-stakeholder processes, with due regard for the diversity of human needs and abilities. Humanity's development and use of the Internet's infrastructure should also be effectively monitored for its impact on our threatened natural environment/s. Furthermore, proposals or initiatives that would serve to "fragment" the global internet--based on inappropriate articulations of "sovereignty", or that primarily advance narrow geo-political interests, run counter to technical efficiency, enforce artificial barriers to global flows of content, and compromise universal access to public knowledge.

3. Freedom of Expression and Association Online

In a global situation where digital content is still denied many citizens and communities for various reasons (e.g.,political, economic, cultural, religious), we reassert that everyone should have the *right to freedom of expression, opinion, and association without interference online and offline*. State and non-state actors should refrain from infringing upon the universal right to receive and impart information, opinions, and ideas. Any restrictions on online activity should conform with *globally accepted principles of necessity, legitimacy, and proportionality*. All laws and regulations that run counter to the aforementioned rights must be responsibly reviewed, revised, and ultimately revoked according to substantial and broadly accepted democratic procedures.

Attempts to silence critical voices and censor social and political content or debate on and through the Internet should be stopped. Everyone should be free to use the Internet *to organize and form associations, engage in legitimate protest, and to freely assert one's identity*. Any moves to advance modes of "digital authoritarianism" on community, national, regional or global levels must be countered in all online spaces where they occur.

4. Open Access to Information, Knowledge, and Culture

We re-emphasize the value of everyone having the *right to access information on the Internet and be free from restrictions on access to knowledge*. Existing copyright and patent regimes must not disproportionately restrict the capacity of the Internet to support public access to knowledge and culture; subsuming the access to life-saving and life-affirming information on the internet, primarily for commercial gain, should be overridden by public interest. Open Access to scientific, research, and academic content must be mainstreamed for the good of all. The production and use of free, *libre*, and open source software (FLOSS)--beyond just primarily artificial and profit-driven intellectual monopolies and artificial enclosures of knowledge--is a key characteristic of an open Internet.

The State, the private sector, and civil society must ensure an enabling environment where *linguistic, religious, and cultural diversity are encouraged and protected*, as these all enrich the development of societies. Arts and culture are part of the invaluable legacy of the Internet, as well as a key channel to its creation, production, distribution, and enjoyment (and a key element to the Internet's original nature beyond commerce or profit). Stakeholders should also continue to promote the *development of local online content* (most especially in local--and particularly endangered--languages) which preserves and enhances heritage, culture, and tradition. *Traditional knowledge systems of indigenous peoples*--long-time targets of commercial exploitation--must also be protected online as offline.

5. Protecting the Digital Public Sphere: Combating Disinformation and Harmful Content

Though the spread of false and misleading content has existed for a long time, and has crossed over to the digital realm from the very start of the 'Internet age', recent history--particularly in the era of big data, powerful algorithms, and ubiquitous platforms--has seen an *unprecedented growth in the sheer volume, velocity, and variety of disinformation*. Beyond just traditional malicious or misleading analog content, the unprecedented platform provided by the Internet and its platforms, coupled with continuing advancements in technologies, have provided malicious actors with ever more sophisticated digital tools and techniques. We vigorously oppose any and all such harmful content and its online proliferation, which serves to *poison the digital public sphere, impoverish our democratic discourse, and compromise further our flawed democracies*.

Increasingly perpetrated not just by individual agents, much of it now originates from syndicated networks of disinformation fueled by powerful actors (State and non-State) with vast financial, human, and technical resources, and deploying the most up-to-date technologies and adaptive A.I. systems). These sophisticated falsehoods--seemlessly using text, audio, and video--seem beyond the reach of existing fact-checking initiatives. We commit to using any and all *technical and non-technical measures to combat this "post-truth" reality* and particularly to *mitigate the numerous real-life risks and actual harms* it poses to targeted individuals and groups, and to the overall digital public sphere.

Other harmful content online--including but not limited to: hate/harmful speech, incitement to violence especially by extremist actors, and the range of vicious digital attacks that demean, defame, and disempower individuals, as well as entire sectors/communities particularly women and societal minorities--must also be addressed via technical, social, and political means.

6. Right to Privacy and the Protection of Personal Data

Everyone has a right to privacy on the Internet and the *right to control how their personal data is collected, generated, and subsequently processed*, even where data is transmitted across national borders and legal jurisdictions. These includes the ability of persons to invoke and exercise their rights as data subjects, as enshrined in the country's data privacy law. Our overly digitized lifestyles and social systems (much of it beyond traditional guardrails of "free, prior, and informed consent") put citizens of the 21st century at unprecedented risk to having our private data and personal identities compromised.

We assert that everyone should be able to communicate online free from unwarranted surveillance and interception. As seen from our experience during the COVID-19 pandemic, targeted surveillance--even when impressed with public interest--must always provide appropriate safeguards and remedial measures, and ought to be governed by transparent rules and oversight mechanisms, with empowered institutions (regulatory and non-regulatory) enforcing them.

Everyone should also have the ri*ght to communicate anonymously* on the Internet and not be prevented from *utilizing encryption and other digital security technologies that ensure unrestricted, secure, and private communication*. Furthermore, the continuing development and deployment of *privacy-enhancing technologies* must be seriously supported by all sectors. Privacy and data protection principles must be *embedded and strengthened within all technical communities and standards-setting bodies*, especially as powerful technologies continue to emerge.

As with many areas in this Declaration, the global footprint and wide-ranging reach of the current big technological companies enable the occurrence of privacy violations on unprecedented levels. The dominant business model is one of maximizing data extraction from its users. On many levels, the "mass" surveillance embedded now in most every program, application, or platform that billions use every day (processed by the most powerful algorithms and computing power), particularly cries out for a strategic transnational effort to counter this effectively.

7. Gender Equality and Addressing Technology-Facilitated Gender-Based Violence

In a situation which still sees less women than men online in many countries of the world, we reiterate that everyone should have an *equal right to learn about, access, define, use, and shape the Internet--regardless of sex, sexual orientation, gender identity and expression*. Efforts to increase universal and meaningful access and use must recognize and redress existing gender inequalities, especially of sexual minorities and gender-diverse groups. In particular, there must be *full participation of women and girls in all their intersectionalities* in every area related to the development of the Internet to ensure gender equality and empowerment.

Gender-based violence involving the use of technology is still prevalent, and the harms and violations perpetrated through and with ICTs are in need of serious attention (particularly the online sexual abuse and exploitation of women and children especially). We reiterate our call for concrete programs and mechanisms to prevent and *address violence in cyberspace* by promoting human rights for all and *harnessing the potential of ICTs to promote women's autonomy, agency, and empowerment*. The Internet must promote diversity and social justice, and should be a *transformative and safe space to challenge and dismantle social injustice and patriarchy*.

8. The 'Digital Economy': Opportunity and Innovation, Equity and Empowerment

The *"digital economy"* is basically the totality of economic activity that is generated by billions of human and technology connections formed online every day. In this regard, everyone should be free to use the Internet for *legitimate commercial activity, value-added innovation, ethical business development, and socio-economic empowerment*. Local innovators/start-ups in particular should be encouraged to design, develop, and implement information and communication technologies (ICTs) that *advance* *socio-economic empowerment and sustainable development*, while contributing to a high-performing Philippine economy enabled by the myriad technologies, applications, and platforms of the global Internet.

The State shall therefore foster a *robust enabling environment for the general welfare of all economic actors, big and small, to participate in and benefit from this digital economy*. Particular measures to ensure the growth of innovators, "techno-preneurs", and start-ups must be encouraged. *Essential anti-trust rules* should be strategic, unequivocal, and realistic to foster genuine competition, prevent monopoly behavior and inorganic market dominance, and protect consumer rights and welfare. Proposals on how to apply any progressive taxation (i.e., "digital tax/es")--especially to the Internet's most dominant players--will be studied and considered, while avoiding unintended consequences of depressing innovation, creativity, and the equitable creation of wealth.

Technological development and rapid global connectivity are spurring on new business models, including the rise of global labor markets. (Online labor platforms show the Philippines as now being one of the major sources of labor supply globally.) More attention must be given to the *workers in this side of the "digital economy"*--including "gig workers" in this current "platform economy", who often constitute its underside. They are the lowly paid, disempowered laborers of the digital age who possess very little rights as workers, but who fuel the prosperity of a small digital economic elite. We support "fair work" and "just labor" initiatives to *advance the interests of those who still do not enjoy traditional workers' rights, including competitive wages, basic welfare benefits, and job security* in the digital economy. (Necessary amendments to our current Labor Relations legal framework to protect these workers may need to be seriously considered.)

9. Human Capital Development: Digital Literacy, Socio-Technical Education and E-learning

Everyone should have the *knowledge and skills that will enable them to access, use, and shape the Internet*. Everyone should have access to online resources, materials, and knowledge. Everyone should have the means to develop their capacity to engage our digital realities, and to steer whatever "digital transformation" is needed according to their and society's benefit. *Digital literacy is fundamental to children's--and indeed adults' as well--capacity to use the Internet competently and exercise their rights.* Beyond this, the continuing evolution of technologies and their varied impacts on people, platform-based institutions, and planet, necessitate lifelong learning (i.e., continuing technical education). This will facilitate more active, responsible, and productive citizen participation in political, social and economic spheres, vastly influenced by online systems.

ICT education--currently situated within our currently flawed (broken?) public educational system--will be of crucial importance if the Philippines is to survive and thrive in the digital present and future. *Human Capital Development for digital citizenship* must be an enabler, and the strategic interventions. Continuing *digital literacy, ladderized socio-technical education, and e-learning*--from formal to informal systems, from basic education to higher learning, from STEM to tech-voc--should be institutionalized. Particular focus on education for e-governance must be integrated into all levels of public sector formation, training and career development.

Specifically, the State and social institutions should promote *open educational resources and enable open access to research and data.* The use of free/open source software and applications in learning environments shall lower cost barriers to citizens, communities, and LGUs. Appropriate user-centric e-learning systems should be developed to accelerate and sustain formal and informal education. *Community centers for digital literacy/e-learning must be present at all local levels*, properly resourced.

10. Promoting Trust, Safety, and Security; Ensuring Liberty on the Internet

Everyone has the *right to liberty on the Internet* and be able to *use it safely and securely*. Everyone has the right to enjoy secure connections to and on the Internet--protected from malware, fraud, and other cybercrimes, as well as applications that threaten or impair the Internet. *The use of technologies and computer resources as weapons to attack persons, communities, and even nation-states* (i.e., cyberwarfare), enabled by or delivered through the Internet and its applications, *must be suspended until such a time when global and national conceptual and operational frameworks shall have been agreed upon* in appropriate and inclusive governance spaces, informed by social and technical assessments of their impact.

Current and evolving threats--fraud, disinformation, online harassment, gender violence, digital manipulation of elections, and the myriad crimes facilitated over the Internet--*must be addressed on multiple levels*: the user, the particular technical platforms involved, and through appropriate protocols and standards emanating from technical and legal communities. These should be strengthened by *legitimate and appropriate legal and regulatory frameworks* that are acceptable to all stakeholders to a safe, secure, and trustworthy Internet.

Cybersecurity policies must be defined through a multi-stakeholder approach, consistent with human rights norms, declarations, and protocols. The deployment of digital security should be proportionate to the threats they are meant to address, taking into consideration the impact of the social, economic and democratic activity they seek to protect.

11. ICTs/Internet and the Environment, Sustainability, & Digital Paths Within the Climate Crisis

The Internet's infrastructure, data centers, data traffic, and end-user devices all have an undeniable environmental impact. This includes ever-increasing energy consumption, greenhouse gas emissions, and e-waste generation--both on our own individual behavior as users and consumers, and on a massive global/industrial scale fueled by the global push for “digital transformation”. Generation of *Waste-Electrical and Electronic Equipment (widely known as WEEE or e-waste)* has been a long-standing Philippine (and global) problem, exacerbated by the country being a transshipment destination of e-waste from other countries as well. *The absence of important regulatory instruments and oversight is glaring and must be addressed*. The Philippine ‘digital society’ is also part of the growing global volume of carbon emissions from the ICT/Internet sector, whose carbon footprint is even greater now than that of the aviation industry. Resource-hungry data centers for example require large amounts of water as coolant to overheating, in a country where potable water is still a luxury for some.

Sustainable use of the Internet and ICTs must be encouraged and enabled, especially as the environmental impacts on people and planet are reaching dangerous--even existential--levels. We must commit to urgent measures that will mitigate this crisis located at the nexus of our digital lives and the Internet’s environmental impact. This includes:

- *Investing in energy-efficient infrastructure*, such as building data centers and networks that use renewable energy sources, and minimizes energy consumption to the greatest extent;

- *Minimization of e-waste and its systemic recycling and/or sustainable disposal* in a manner that is protective of the environment, with *extended producer responsibility (EPR)* measures established and enforced;
- *Promoting sustainable device* use by encouraging consumers to use energy-efficient devices and engaging in responsible e-waste disposal;
- *Including environmental education in digital literacy programs* to equip people with the skills to use the internet safely and responsibly, while reducing the environmental impact of their online activities.

Moving away from the current consumeristic consumption patterns of 21st century digital capitalism is paramount.

10. Platform Governance: Addressing Gross Power Imbalances in Digital Societies

In today's digital age, *the pervasive influence of digital platforms is undeniable*. In 2023, 60% of the global population, or 4.75 billion people, were on social media platforms owned by a handful of private internet companies, which are among the richest in the world. These platforms are sites of a multitude of online activities beyond just social interaction--they now cut across almost all strategic and economically significant industries, including banking and commerce; transport and mobility, retail and entertainment, health and lifestyle. They are innovative, aggressive, disruptive--and they concentrate digital power like never before.

Big Tech companies wield significant market power, advancing commercial models which are highly profitable, but ethically problematic: they regularly bypass competition, subvert labor and privacy rights, and implement flawed content policies which privilege negative content. The algorithms behind their content curation and moderation systems are not publicly transparent, and pose risks to the digital public sphere. Their practices constantly challenge under-capacitated regulators and policymakers. Similar to authoritarian State actors, platforms also thrive on the unauthorized extraction of user data, and deploy advanced technologies which result in greater control of their user experience of their “free” services. These practices serve to disempower the majority of users and diminish their autonomy and agency, further exacerbating existing inequalities in society.

To counteract this trend, it is crucial to recalibrate our frameworks of what our digital societies have evolved into and what they should be. We must *assert ethical guardrails to defend rights, safeguard the digital commons, and disperse power equitably and democratically*. Democratic governments and civil societies must be assertive in *policing the platforms through different modes of regulation*. Civil society must continue to *engage the networks* in behalf of people who remain in them. This engagement could range from regular dialogue and democratic debate, to applying pressure on the platforms into complying with human rights practices and protocols. Civil Society actors and regulators may also utilize str*ategic litigation* to establish legal precedents against clear anti-trust, privacy, or content moderation violations.

Other suggested measures to push for include: more responsive and culturally-sensitive content moderation; requirement of platforms for greater transparency--algorithmic transparency for one, financial transparency as well on their financing--and better risk assessments; the establishment of independent third party regulators and oversight boards.

As advanced by numerous multi-stakeholder forums and UN agencies (i.e., UNESCO), we must demand that digital platforms comply with the following key principles:

- Platforms conduct human rights due diligence, assessing their human rights impact (including gender and cultural dimensions), evaluating the risks, and defining the mitigation measures.

- Platforms adhere to international human rights standards, including in platform design, content moderation, and content curation. Platforms should follow relevant international human rights standards, including the UN Guiding Principles on Business and Human Rights. Design should ensure non-discrimination and equal treatment, and that harm is prevented; content moderation and curation policies and practices should also be consistent with HR standards, whether these practices are implemented through automated or human means, with knowledge of local languages and linguistic context, as well as respect for cultural diversity, and adequate protection and support for human moderators.

- Platforms are transparent and open about how they operate, with understandable and auditable policies as well as multistakeholder-designed metrics for evaluating performance. This includes transparency about the tools, systems, and processes used to moderate and curate content on their platforms, including in regard to algorithmic decisions and the results they produce.

- Platforms make information accessible for users to understand the different products, services, and tools provided, and to make informed decisions about the content they share and consume. Platforms provide information and enable users' actions in their own languages and consider users' age and disabilities.

- Platforms are accountable to relevant stakeholders—including users, the public, and actors within the governance system (e.g., policy-makers, regulators)—in implementing their terms of service and content policies. They give users the ability to seek appropriate and timely redress against content-related decisions, including both users whose content was taken down or moderated, and users who have made complaints about content.

We believe the internet is a transformative space, where individuals can exercise their rights and express themselves, no matter their social standing or economic class, gender or sexual identity, religious or ideological beliefs. It is a space where anyone can communicate with everyone--especially the people they love, cherish, and respect. It is a space where one can engage the world and participate in political, economic and social life. It must be defended from malicious actors, digital authoritarians, cyber-monopolists, and others who abuse the Internet, exploit its applications, products, and services in inauthentic and unethical ways.

We will thus defend the Internet as a free, open, collaborative, and liberating space. This is the Internet we want. This is the Internet we deserve. **This is the Internet we will fight for.**

###

SIGNATORIES:

CROSS-CUTTING AREAS OF CONCERN

A. EFFECTIVE/EQUITABLE E-HEALTH SYSTEMS (IN AND BEYOND PANDEMICS)

Health is an important social system, but it also in and of itself a human right. In this age of pandemics which challenge our health systems, digitalization within health systems is integral--not only to saving lives and mitigating of harms--but is an important enabler of and lifeline to social, economic, and political adaptation. The recent COVID 19 pandemic was also a mirror wherein we experienced the real implications and impacts of an accelerated digital migration, but also our (un)readiness and our (in)capacities to do so. It revealed very real gaps in our health systems, and indicated as well as how human rights were (mis)treated during the State's pandemic response. We need to ensure that even in an emergency setting where the general public health interest is paramount, human rights must always be respected and upheld. As e-health becomes more ubiquitous and necessary to citizens and communities, the lack of a strong Human Rights frame puts stakeholders at further risk. We must use ICTs and the Internet to build a more equitable and responsive e-health system.
As an initial response, our e-health systems should "Mind the GAPS, fill the G.A.P.S." (as articulated by the Asian E-Health Information Network/AEHIN):

GOVERNANCE. We call on governments to create *accountability structures* that will enable the development of national digital health strategies responsive to the complexities of pandemic response (and beyond). Using our COVID experience, this would necessarily include data governance, aside from disease surveillance, testing, contact tracing, quarantine management, and clinical care--all digitally enabled, enhanced, and executed. The Department of Health (DoH) shall cultivate a conducive environment for the formation of public-private partnerships to foster much-needed collaboration.

ARCHITECTURE. Data-sharing during pandemics is complex and requires pro-active engagement to coordinate the work of different stakeholders within and across borders. To enable secure data sharing, countries are encouraged to share a clear *interoperability architecture* (or blueprint at the very least) for adoption by all. This blueprint should be useful for COVID-19 and for other health programs of the DoH and other stakeholders.

PEOPLE / PROGRAM MANAGEMENT. All stakeholders should support the effort to *strengthen the capacity and capability of our national eHealth staff and leadership*. This includes developing capacity within DoH to manage digital health-related projects within the agency and also in partnership with other sectors--leveraging local, regional, and global learning networks to *catalyze knowledge exchange* across different countries in the Philippines and elsewhere.

STANDARDS AND INTEROPERABILITY. We will promote open access and require technical assistance to effectively adhere to international health/data standards, which are crucial components of the interoperability blueprint, and will enable the availability of health data for better monitoring of population health.

We also will continue to fight for all our aspirations for the health and wellness of our communities, our nation, as well as the global community. Health is a human right, and the foundation which enables the enjoyment of all other rights. The internet should be a positive force for good which brings us closer to our envisioned reality.

#

B. ICT SYSTEMS AND ELECTORAL INTEGRITY: SOME INITIAL CONSIDERATIONS

Elections and related electoral exercises--like all other societal systems--are undergoing rapid digital shifts, with new and emerging technologies promising many benefits, but may also represent new threats, particularly in the Philippine context. In the area of ICT systems and elections, it is primarily the responsibility of the State to ensure that technical measures and security mechanisms are in place to protect the right of every citizen to participate in electoral exercises to exercise the right of suffrage, regardless of the technologies used. But all stakeholders must work to ensure that the integrity of the elections is not compromised, and trust in digitally-enabled electoral processes is built and maintained.

CONTEXT

Constitutional and Legal Mandates. The Constitution (Article IXc) and the Omnibus Election Code (Section 42) both state that elections should be “free, orderly, honest, peaceful, and credible”. The Automated Election Law (RA 8436, as amended by RA 9369) further declares, *“It is the policy of the State to ensure free, orderly, honest, peaceful, credible and informed elections, plebiscites, referenda, recall and other similar electoral exercises by improving on the election process and adopting systems, which shall involve the use of an* ***automated election system that will ensure the secrecy and sanctity of the ballot and all election, consolidation and transmission documents in order that the process shall be transparent and credible and that the results shall be fast, accurate and reflective of the genuine will of the people.****”*

The AES and Its Discontents. Since 2010, the Philippines has been implementing an Automated Election System (AES) that has periodically caused concern with numerous groups. Challenges have been raised as to its technical aspects, centering on how the electorate (unlike in the old manual system) has been excluded in participating in the processes of vote counting and canvassing in favor of vote-counting machines and automated transmission of results. This has been questioned for its perceived lack of transparency.

The most recent 2022 National and Local Elections showed that the majority of the voters are fairly confident with automation, and trust in the system seems relatively high. The main concern however of those questioning the recent AES implementation centers on the lack of transparency in the counting and canvassing, leading to mistrust in the ultimate results from certain quarters. There have been calls for processes which again allow voters to observe these important aspects of the election, in an open, transparent, and understandable way.

Elections should not be technically complicated, and the same results should be achieved by improving previously manual processes through technology. There should be no monopoly in knowledge when it comes to the AES processes, nor should the actual operations be reliant on just one specific group (or technology provider). (Note: electoral automation encompasses many aspects--e.g, voter registration, voter identification, management of the voting procedure, data privacy/security, etc.)

What should be done then to build back the trust and confidence in the integrity of automated elections--particularly in vote-counting and the transmission of results? Some considerations include:

Some Guiding Principles for Automated Elections (adapted from NAMFREL 2022)

- **Technology-Agnosticism**. Any automated election should not be reliant on a specific technology or method. Automated election systems should adapt to what is available, affordable and appropriate.

- **‘Private Voting, Public Counting’**. This is what the constitution prescribes in terms of data management. The entire design and implementation of any automated system should make sure to protect the privacy and security of voter’s information, as well as the voter’s ballot. There should be no direct way of tracing a ballot directly back to a specific voter (i.e., private voting). However, the content of the ballot, even on an individual voter's level, should be made available to the public. As such, any summary of how the voting went--such as through an election return (ER) or a certificate of canvas (COC)--should be made available to the public (i.e., public counting).

- **Open Data format.** All data exposed to the public--from the individual ballot to all summarized forms (ERs and COCs)--should be available to the public in a format that is also publicly available. The data should also be easily accessible using the latest available technology without the need for specialized hardware or software. The data should also be present in at least two redundant formats--a machine-readable one and a human readable one. (This follows a similar principle in accounting of doing T-entry or Double-entry to have an atomic self-check.)

- **Digital Signatures.** The signature which appears on the summarized forms such as the ERs and COCs must be the digital signature of/by the authorized Election Boards (EBs) that are independently generated through a national Public Key Infrastructure (PKI) facility. The signature must be verifiable and traceable to an individual person. This ideally follows the private-public key security mechanism in which the private key is only known to the EB.

- **In-Precinct Count and Audit.** Using the machine-readable portion of the ballot, an in-precinct summarization of the votes and the generation of the summary ER must be done after poll closing and in-precinct. This should be done immediately after closing of the polls with the ballots shared to independent accredited groups for their own verification. This is critical as this is the source information of data for that particular election. This is the elemental data source that can be summarized to generate results up to the national level, and later audited.

OTHER TECHNICAL MEASURES.

All these will be operationalized in conjunction with other **technical guidelines and safeguards** including (but not limited to):

- Pre-election election software Source Code Reviews;
- Random Manual Audits of election returns and election machines;
- Updating of rules on Election Spending (that will cover digital money transfers/e-wallets/ exchange of digital currencies, and other analogous financial technologies);
- State of the art cybersecurity measures to protect against illegal interception of electoral data.

The **right of suffrage** is one of the most respected rights of the Filipino people, and we must work towards defending and extending this right as enabled by ICTS and the Internet. The Right to Suffrage must extend to cyberspace and the digital age!

###

C. The Challenge of Artificial Intelligence

WHAT IS AN ARTIFICIAL INTELLIGENCE (A.I.) SYSTEM?

An A.I. system is a machine-based system designed to operate with..levels of autonomy, and that may exhibit adaptiveness after deployment... It infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. (EU A.I. Act);

The simulation of human intelligence processes by machines or computer systems

POTENTIAL AND PERIL

Artificial intelligence is a fast-evolving family of technologies that is seen to contribute to a wide array of economic, environmental, and societal benefits across the entire spectrum of industries, sectors, and social activities. By improving prediction capacities, optimizing operations and resource allocation, and personalizing digital solutions available to individuals and organizations, the use of artificial intelligence (A.I.) has been proven to support socially and environmentally beneficial outcomes (e.g., healthcare, farming and rural development, climate change mitigation/adaptation, among many spheres), while also providing key competitive advantages to businesses.

At the same time, depending on the circumstances regarding its particular application, context and mode of use, level of technological development, and even its specific design, artificial intelligence may generate risks and cause harm to the public interest, as well as to fundamental rights. Such harms might be material or immaterial, including physical, psychological, social, political, or economic harm (e.g., human job loss, algorithmic biases/discrimination; invasion of privacy, undermining of due process, automated weaponization; or simply its propensity to "hallucinate" when giving answers to real-life human questions). Digital Rights advocates have pointed out actual and potential risks of A.I. systems to human rights, and even a broad spectrum of technologists--creators, designers, and developers of A.I. systems themselves--have openly advocated for a "pause" in massive A.I. systems development and deployments. Many of these recommendations are underpinned by significant ethical considerations, as the adaptive nature of the latest models of A.I. applications make it seem like a Frankenstein-like creature or Pandora's Bo--which no one has fully grasped the full implications and impact of. From school-level plagiarism of content, to potentially catastrophic A.I.-enabled global cyberwarfare, it is definitely at the center of this century's important existential questions.

As such, most of the big players in technology have already invested billions of dollars in A.I. development, believing that this is the proverbial "technological killer app" that will ensure wealth, dominance, and power now and in the future. Almost all governments are doing the same for a broad spectrum of reasons: business development, and economic investment; politics, governance, and geopolitical advantage, or the promise of development outcomes. Individuals are also trying out the limits and possibilities of A.I.--mainly through publicly available chatbots--in many spheres and contexts, both for work and play. (ChatGPT--a generative A.I. interface emblematic the power of the technology has the public eager to test out the groundbreaking technology at the personal and professional level--it is now reportedly the fastest-growing app in history.)

The enigma has always been--how to properly engage A.I.?

HOW TO HARNESS, HOW TO GOVERN?

As Big Tech and smaller economic players, technologists, entrepreneurs, policymakers and all who have a stake in the digital future go all in with their A.I. investments, and nations rush to develop roadmaps and earmark resources in what seems like a digital “gold rush” to deploy A.I. applications, it is imperative that all stakeholders understand the discourse in order to participate in shaping A.I.’s future.

Many of the emerging frameworks--ethical, economic, political, socio-technical--revolve around the theme of a desired “human-centered” A.I. at the core of the desire to govern it properly. Part of many numerous frameworks tend to include these examples of regulatory handles for A.I.:
a. Evolution of appropriate technical guidelines and standards for general-purpose and specific A.I. applications;
b. Stricter development and deployment guidelines for large-scale applications, including more meticulous testing;
c. Ensuring the mitigation of algorithmic bias and discrimination in the design of A.I. systems;
d. Increased transparency/disclosure requirements;
e. Enhanced data protection mechanisms to ensure privacy rights are upheld;
f. Pro-active prevention of Malicious AI Use;
g. Accountability for A.I. security incidents/harmful impacts
h. Certification and Compliance Audits

ENGAGEMENT TO EMPOWERMENT

Joint research initiatives and greater collaboration in A.I. development seems to be a good starting point. Different stakeholder communities are acknowledging more and more the need for certain “guidelines and guardrails” to be adopted in order to maximize benefit and minimize risk. Many of the voices still preach strategic ENGAGEMENT, rather than ignoring its potential impact. On the technical side, designing and deciphering possible applications in the ENGINEERING and technological development space; as with other levels the need for more transparency will benefit the public good. A.I. literacy is deemed indispensable for intelligent discussions and debates my more people impacted by it, so continuiing A.I. EDUCATION on all levels is a must. ETHICAL considerations must be paramount in assessing the actual and potential impact assessments. EFFECTIVE GOVERNANCE, including strong ENFORCEMENT capacity for the agreed-upon governance handles is key. And it should all lead to greater EMPOWERMENT of citizens and communities, and not the other way around.

A Civil Society A.I. Study and Working Group must be convened at the soonest possible time to further assess and explore the developmental implications of such a game-changing technology.

###