EDUCATIONAL RESOURCE GUIDE TO THE *CHARTER OF HUMAN RIGHTS AND PRINCIPLES FOR THE INTERNET*
2016

Educational Resource Guide

School of Information Studies
Syracuse University 2016

Internet Rights & Principles Coalition

The views expressed in this document are those of the authors and do not necessarily represent the views of the Internet Governance Forum or the Internet Rights and Principles Coalition.

Authors:
Allison Baker, Gabrielle Cohen, Bianca Concepcion, Alexis DeMarco, Victor Garcia Jr.. Elan Heller, Fanli Ji, Josue Luna, Khadija Malik, Tim Marston, Peter Menaker, Taylor Murphy, Jason Stein, and Wan Zhang

Acknowledgements:
The educational resource guide to The Charter of Human Rights and Principles for the Internet was made possible by undergraduate and graduate students from the School of Information Studies at Syracuse University.

Thanks should be given to Professor Lee McKnight, who taught IST 456 and IST 728. Without his guidance, this project may have never existed or developed to what it has become today.

INTRODUCTION

In Fall 2015, the students of Dr. Lee McKnight's Information Policy and Decision Making undergraduate course set out to learn more about the Internet Governance Forum (IGF). Through contacts, it was discovered that an educational resource guide for the Charter of Human Rights and Principles for the Internet was needed. This educational resource guide would act as a study guide for anyone who wants to know more about the charter or a specific principle. After several semesters, a final draft of the study guide was established. This effort was divided amongst a combination of undergraduate, graduate, and law students.

To complement the educational resource guide's creation, Syracuse University hosted a remote hub for the Internet Governance Forum Conference in both 2015 and 2016. The students that worked on this project were recognized for their effort at the 2015 remote hub, and were also the only remote hub on a college campus in the United States.

Going forward, this document outlines and breaks down each of the 20 principles outlined in the charter to help readers more clearly understand and interpret them. At the end of each section, there are external resources that the reader can use to find out more information about each topic. The end of this document also has a list of legal cases to reference for further clarification.

TABLE OF CONTENT

1. RIGHT TO ACCESS THE INTERNET

Growth in the number of Internet users in the world indicates the proliferation of Internet Service Providers. Every Internet user should have the right to access an adequate quality of service that is feasible through current technological developments.

Open standards enable Internet users to have a greater variety of options. An example of this is the difference between the Android and iOS market for mobile applications. Users have the freedom of choice for different systems and software.

A form of digital inclusion that is common in many countries is publicly accessible points of Internet access. In the United States, these are most common in public libraries, clinics and schools. A 2013 study published in the Journal of Community Informatics provides an overview of these “public internet access points” in Africa, Europe, South America, North America, Australia and Southeast Asia.

In addition, net neutrality and net equality has been a popular topic in both Europe and the United States recently. In June 2015, the U.S. Federal Communications Commission published an “Open Internet Order”, which ensured that consumers and businesses have access to a fast, fair, and open Internet. Three key rules were laid out: 1) no blocking of legal content 2) no throttling of Internet traffic based on the content being accessed, and 3) no paid prioritization of content based on a fee structure. In October 2015, the first EU-wide Net Neutrality laws were passed and enforced in April 2016. These laws ensure that the same provisions apply across Europe, which includes no blocking, throttling, or discrimination of online content, applications and services.

External Resources:

An Analysis Of Public Internet Access Points (PIAPs)
U.S. Federal Communications Commission Open Internet Order
Agenda for Europe (EU) – Net Neutrality

2. RIGHT TO NON-DISCRIMINATION IN INTERNET ACCESS, USE & GOVERNANCE

Each person on the Internet is entitled to rights regardless of their: ethnicity, skin color, sexual identity, language, religion, political. On the Internet we should all enjoy the same rights and freedom. This also extends to the right to have access to the Internet. Groups in society have been given different levels of access to technology and the Internet. In order to make the Internet less discriminatory, people must have access to the Internet. This will give marginalized groups, such as elderly or ethnic or linguistic groups, a voice and way to have access to the tools they need. A person on the Internet should not be limited by their born gender or the gender they identify with. These limitations will foster discrimination if all people are not given the same rights.

"Gamergate" is an online movement that was established by *Firefly* actor Adam Baldwin. Baldwin created this hashtag on Twitter to help bring awareness to the corrupted field of game journalism. Game journalists and game developers maintain close friendships and relationships causing the work that the journalists to be questioned as bias. Another focal point of "Gamergate" is concerned with protecting the "gamer" identity. The "gamer" identity applies to millions of users gaming in real time with other gamers on the network. The actions taken by users online can have a detrimental effect on a person's real life and their wellbeing. "Gamergate" is focused mainly on the journalistic ethics and user identity protection in the gaming world.

#Gamergate began in early August 2014 as an attack on a female game developer, Zoe Quinn. Quinn had been the victim of death threats and harassment since the time she began trying to publish her text-based game: Depression Quest. The harassment began on 4chan, a discussion-board website. As a response, Quinn's ex-boyfriend, Eron Gjoni, wrote a series of blog posts stating that Quinn had cheated on him with five other individuals. These individuals were all associated with game journalism as well. From there, various gamers in different social circles online concluded that Quinn had used those five male individuals to gain publicity for her game. Anonymous users then harassed Quinn's morals and lifestyle on a public discussion board.

For a long period of time, Zoe Quinn received threats of different kinds from rape to assault or death. Her personal information was published online such as her phone number and address. The situation escalated to the point where Quinn no longer felt safe in her own home. According to the New York Times, Quinn proceeded to stay with different friends to avoid being stalked.

Due to this incident with Quinn alongside many others, the Internet Governance Forum planned an Anti-Cyber Violence campaign resulting from the events of #Gamergate.

External Resources:

Indiana University study on Internet use by marginalized groups
Washington Post article on GamerGate
Zoe Quinn's Depression Quest

3. RIGHT TO LIBERTY & SECURITY ON THE INTERNET

Security is the utmost importance, no matter what form. With rapidly emerging and morphing technology, this topic can be controversial on what security means in relation to the Internet. This principle highlights that measures will be considered illegal when they infringe or restrict another human right. This is a general consensus, except in extenuating circumstances. Ways that the Internet could infringe on human rights can be interpreted in many different ways depending on whom you speak to. According to Alexander Howard, Governments are trying to pressure technology companies in to creating a back door to "provide access to encrypted information". Encryption helps protect billions of users personal information from privacy threats, and allows users to have liberty and freedom when it comes to Internet usage.

Today, many tools are being developed to protect personal information. These tools are referred to as privacy enhancing technologies (PET) (pg. 2-3, Weber). The fulfillment of customer privacy requirements are difficult to implement because we are living in a time where hackers are only getting smarter, and their tools are getting stronger. Some of the PET's that have been developed are virtual private networks (VPN), transport layer security (TLS), DNS security extensions (DNSSEC), onion routing, and private information retrieval (PIR).

One can see that many of the tools do not guarantee full protection. According to the article, "Securing the Internet of Things", developers are creating a worldwide object in which they must build an infrastructure that allows mutual object authentication. This will ensure that the Institute of IOF is practicing transparency, where users know which entities are managing their data.

Total security and protection against all forms of crime are necessary steps to ensure the security of every global citizen whether they use the Internet, or not.

External Resources:

Alexander Howard
EU/Council of Europe Project on Global Action on Cybercrime (GLACY)
Convention on Cybercrime ("Budapest Convention")
OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity

4. RIGHT TO DEVELOPMENT THROUGH THE INTERNET

Everyone has a right to the Internet. Students can do better in school, people are able to gain newfound skills, as well as acquire knowledge that would take much longer to learn. But the problem with this is there is good fraction of the world that has yet to be connected. Society must find a way to connect people in struggling nations, in order to bring them up to speed to the rest of the world. In a report by the International Development Research Centre states that policies must be enforced in Latin America in order to regulate a nation-wide broadband that can help the connectivity issues of 3rd world countries. Countries such as these would have more accurate weather predictions, access to online textbooks, as well as the ability to connect and communicate with the online citizens of the world. Internet and cellular coverage is available, but it is too expensive for people to afford. Initiatives like Free Basics by Facebook, partner up with some of these mobile operators to provide access to websites, for free. Now while this does address the issue, it is just a momentary fix. Permanent solutions must be implemented to help these countries develop in the long run.

As well as aiding the developing nations our environment requires attention of equal importance. The rapid pace of development must be matched with policies that concern the harmful components that these devices produce.

Computer processors contain several harmful elements like lead and mercury. Both of these damage plants and animals that may come into contact with e-waste. In the U.S. alone in 2012 there was about 3.4 million tons of e-waste generated with only 29.2% recycled. What remained was tossed in landfills or incinerated, which does not safely dispose of the toxic materials within the electronics. In addition, recycling these electronics means being able to re-incorporate some of the more valuable components like gold back into the market.

External Resources:

The Internet and Poverty: Opening the Black Box
Internet.org
How Clean is your Cloud?
E-Waste

5. FREEDOM OF EXPRESSION & INFORMATION ON THE INTERNET

With the Internet as a breeding ground for all types of information, a person can find almost anything that they inquire to know. According to the Charter of Human Rights and Principles for the Internet, the 5 freedoms of expression and information on the Internet are: freedom of online protest, freedom of censorship, right to information, freedom of the media, and freedom from hate speech.

Freedom of online protesting involves the right of using the Internet to be involved in online and offline protests. Freedom from censorship involves having the right of doing what one wants without any forbiddance. For example, users have the freedom from cyber attacks as well as online harassment. This part of freedom of expression also includes the freedom from blocking and filtering. Internet companies have no rights to hide content, express information about Internet users, and remove content.

The right to information includes everyone having the right to look up, receive, and convey information and ideas through the Internet. This means that everyone has the right to connect in order to make effective use of government information due to national and international law. Freedom of the media communicates that everyone should respect other people's media. An example of this: no one has the permission to plagiarize or rather copy another person's work, especially when it is copyrighted or it is against the law. Freedoms from hate speech means that everyone's opinions must be respected. Article 20 of the ICCPR is an example of this. People thinking they have the right to express whatever they feel can lead to others injuring themselves due to racist/bias comments.

This freedom can come with major consequences and side effects if there are no restrictions put in place. Some of the consequences of freedom of expression and information are: the rights of others, protection of national security, or for someone's mental health. Article 20 of the ICCPR shows how everyone has to respect each other's opinions. It states that no one can be racist or show religious hatred that involves discrimination, or violence otherwise the law will forbid it. Therefore, since the Internet is such an important aspect to our society, the Internet also has its own set of rules for freedom of expression.

External Resources:

Internet Censorship and Surveillance by Country
Open Net Initiative
Reporters without Borders
Facebook Statement on Hate Speech

6. FREEDOM OF RELIGION & BELIEF ON THE INTERNET

It is essential to maintain freedom of religion on the Internet. Currently, there are many issues throughout the world that prevent some religions from expressing themselves on the Internet. This principle is extremely important in current day society due to the increase of connectivity throughout the world. Online religions are becoming more prevalent throughout society. The international community needs to come together to ensure that religions have the right to demonstrate safely on the Internet.

One major blockade that exists is government restrictions on certain webpages. Country leaders tend to block websites that go against personal beliefs or country initiatives. An example is Saudi Arabia's strict definition of the state's official religion, Sunni Islam. In the US Government's International Religious Freedom Report, The Committee for the Promotion of Virtue and the Prevention of Vice reported that over 20,000 websites have been blocked by Saudi Arabia. One specific example occurred in April 2014 when a court of appeals forced the Liberal Saudi Network to shut down. It was revealed that this action occurred due to the network discussing political and religious topics. These constant website shut downs is a clear violation of religious freedom principles. Under to the principles of the charter, Saudi Arabia must adapt to international standards and allow a healthy debate and discussion in regards to religion.

Another major development is the rise of the cyber religions. People exclusively practice their religion on an online platform. For example a virtual church named The Church of Fools had a user log in as the Satin and post malicious comments. This type of spiteful action happens multiple times a day across different platforms. It is necessary to allow freedom of speech on the Internet while enabling online religions to practice in a safe environment. In order to allow this, there needs to be protection from malevolent people whose objective is to disrupt and persecute cyber religions.

External Resources:

Saudi Arabia 2014 International Religious Freedom Report
Virtual Church Forced to Tighten Security
Online Religion as Lived Religion

7. FREEDOM OF ONLINE ASSEMBLY & ASSOCIATION

Today on the Internet, it is very easy to make groups and associations through many social media sites. Many people communicate on groups through Facebook, Twitter, and many different online forums. Because of this act, all of the Internet contexts of groups must be peacefully protected when talking in the group. In a political sense, all protests are planned and organized through the Internet. The Internet has become an easy way for large groups, especially under short notice, to communicate with each other.

The Freedom of Online Assembly & Association correlates closely with The Freedom of Expression on the Internet. They both have to do with joining groups and having the right to say how they feel within the associations. The freedom to associate and assemble communities on the Internet must be protected for the people to organize their voice. Any party must have the right to express their views and be able to connect with online communities without filters, blocks, or any other forms of censorship. No one may be compelled to join any organization or group if they do not permit it. This is the freedom to choose and join any online group through one's own volition.

An example of Freedom of Association is the Turkish government's blocking of Twitter. Why did Turkey block Twitter? The Turkish Prime Minister thinks, "social media is the worst menace to society." This is due to many people talking badly about race, sexuality, religion, etc. Twitter is a social media website that in the end can really hurt people. However, due to many years of this governance, members of society have figured out a way to bypass the blocking of Twitter.

External Resources:

Turkey blocking Twitter and other social media sites

8. RIGHT TO PRIVACY ON THE INTERNET

Everyone has the right to the protection from interference or attacks, even on the Internet. The Internet of Things (IoT) is trying to promote innovation, while balancing privacy and security at the same time. There will be an introduction of billions of nodes on the Internet and users will be able to connect virtually anywhere they go. In order for Internet users to be able to communicate on any platform anywhere, user information will be more transparent than ever. With the development and ideation of IoT, security applications and features need to be simple and easily understood by all users in order to protect personal information. Security platforms need to be available to users but in a way that they have full accessibility to their own data and have the decision making power of what is available to the public.

With technology nowadays, most information can be find online. However, everyone shall have the right to privacy on the Internet. According to the Charter of Human Rights and Principles for the Internet, states shall consider the right of privacy on the Internet to be equal to other international human rights and must be protected under government laws. Privacy policy setting for online activities shall be easy to find with understandable content for users to avoid confusion and future problems.

Furthermore, there shall be standards for confidentiality and integrity of the IT-system. Everyone shall have the right to protection of personal data from being monitored, tracked, or profiled, etc. Additionally, PIN and TAN codes must not be used and changed by others without permission of the owner. Individuals have the right to ensure security and privacy by using encryption technology and anonymous communication. Everyone shall have the right to protection his or her honor and reputation on the Internet.

External Resources:

Visualization of different national data privacy laws
UN report on the promotion and protection of the right to freedom of opinion and expression
Anonymity and the freedom of expression

9. RIGHT TO DIGITAL DATA PROTECTION

“Anonymous” is the Internet hacker group responsible for several data breaches, most notably the Ashley Madison case. This is a great example of right to digital data protection as well as the right to consumer protection on the Internet. When users sign up for social media sites, they are in control of what information is available and, in the case of Ashley Madison, whether or not to pay for increased security. Millions of users had their personal information, including addresses and phone numbers, posted online for users to access. Identity fraud is an increasingly important issue, especially now, since information can be easily accessed on the Internet. Is there a way to protect information once it is released? How will those users be protected against identity fraud?

The recent ruling by the European Court of Justice on the validity of the Safe Harbor Principles highlights the growing level of accountability of data collectors, who are concerned about the personal data they store by their customers. Data collectors operate in various regions in the world expect a different set of obligations, which can be challenging when data moves in and out of national jurisdictions.

A reform of data protection rules in the EU was proposed in January 2012, while in May 2016, the official texts of the Regulation and the Directive have been published in the EU Official journal. The Regulation and Directive both shall be applied and transposed into national law by May 2018. Under the EU law, personal data can only be collect for legal purposes and must be protected from misuse, and certain rights of the data owners must be respected.
There is currently no global minimum standard on the use of personal data. Standards vary by country, with the greatest level of data protection being administered through the European Union. The lack of globally accepted standards for use of personal data poses a challenge to large Internet-based companies, as they must carry out global operations amidst various personal data standards.

There are numerous data protection authorities in Europe (France, Germany, Ireland, Sweden, UK, and Norway). However, most countries do not have a formal “date protection authority”. These public organizations could serve as liaisons among each other to promote better global data protection standards and international cooperation.

External Resources:
Europe vs. Facebook
Overview of Safe Harbor Principles
EU Data Protection Authorities
EU Right to be Forgotten factsheet
EU Protection of personal data

10. RIGHT TO EDUCATION ON & ABOUT THE INTERNET

Education is a helpful tool for many people to fulfill their goals and aspirations in life, regardless of their location. The Internet can be instrumental in providing education to any part of the world because it can be tailored to any language, pedagogy and knowledge-traditions. Self-organizing learning environments (SOLEs), such as Khan Academy, can be a solution to many problems. SOLEs can give access to individuals that need extra attention on a topic or want to educate themselves on a particular topic.

In this setting children form groups, acquire and demonstrate the skills of ideation, broad-frame pattern recognition, and complex communication. This can restructure their learning to what works well for them and help establish independent learning methods. The students who are fortunate enough to participate in these SOLEs have better communication skills and are more likely to have innovative thoughts and ideas. This is based off Sugata Mitra's experience creating these "schools" in India where they're working well. This SOLE experience is giving people the skills that are advantageous over digital labor.
Devices and Technology are getting introduced to children at a young school age, and for some children it starts before they begin school. SOLEs can help develop and master a child's digital literacy.
With the increased use of technology in the classrooms, the educational system owes children the basic knowledge of how to conduct themselves online, basic Internet uses, and their human rights on the Internet. Children need to be socialized to the environments that exist on the Internet. All human rights should be acknowledged and respected in the same way you would communicate with someone in person. However, there is a gap in education so there are children who don't know how to act respectfully on the Internet. Unfortunately, some children grow up thinking, that the screen separates them from the rest of the world that they are communicating with and that there are no consequences for their actions.
Children need to know that they screen cannot and will not protect them from the consequences of their actions. People should treat others as they would want to be treated over the Internet. Now more than ever, other children on the Internet are bullying children. This is a problem that has taken many lives but can be addressed with education of the Internet human rights.
There is also a gap in parent and child knowledge of the Internet and technology. Children are now more knowledgeable of the Internet and technology than their parents. Parents need to take the initiative to learn how to raise their children on their rights and behavior on the Internet. The Internet can be a great tool for children to educate themselves on their interest but the Internet should not be a place where they are bullied.

External Resources:
Children and the Internet
Children's Rights in the Digital World

11. RIGHT TO CULTURE & ACCESS TO KNOWLEDGE ON THE INTERNET

Every Internet user should have the right to participate in the cultural life of their community. As well as, the right to use his or her own language, the freedom from restrictions of access to knowledge by licensing and copyright. The Internet shall also represent a diversity of cultures and languages, knowledge commons and the public domains. Promoting the cultural and linguistic diversity on the Internet benefits the Internet a diversity of cultures and languages in terms of appearance and functionality. For example, Internet Corporation for Assigned Names and Numbers (ICANN) has announced its first new generic Top-Level Domains (gTLDs) on October 2013, which indicates that the Internet Domain Name has been expanded from 22 gTLDs to nearly 1,400 new names or "strings." Moreover, the new gTLD program has introduced non-Latin scripts such as Arabic, Chinese, Greek and Hindi for the first time. "The delegation of non-Latin script gTLDs demonstrates ICANN's efforts to create a globally-inclusive Internet, regardless of language or region. Making open standards and open formats available has made the Internet a better place for people from all over the world to collaborate effectively and efficiently. One of the great examples is Github, which is the world's largest open source community that allows users from different countries and cultural background to collaborate virtually on the platform. It provides free services to both personal and organizational users. Github has become a hot tool for global teams and programmers to deliver their projects. The collaborative community on Github can provide a safe space for individuals all over the world to improve current software issues or needs.

External Resources:

ICANN New Generic Top-Level Domains in Arabic, Cyrillic & Chinese
Creative Commons
GitHub
Overview of WTO TRIPS Agreement
Teaching Copyright

12. RIGHTS OF CHILDREN AND THE INTERNET

In terms of children and the Internet, children must be given the freedom to use the Internet. In addition, they should be protected from the dangers associated with the Internet. The balance between these two priorities should depend on the child's capabilities. Governments must respect the rights and responsibilities of parents and extended family to provide guidance for the child based on the child's evolving capacities. Some of these evolving capacities may include: right to benefit from the internet, freedom from exploitation and child abuse imagery, right to have views heard and lastly, best interests of the child. In freedom from exploitation and child abuse imagery, children have a right to grow up and develop in a safe environment that is free from sexual or any other kinds of exploitation or abuse. There are often stories on the news of a child pornography being produced or distributed online. In October 2015, FBI-issued spyware led to an arrest of a child pornography suspect. A special agent in the FBI testified a complaint that a Tor-based website called "Playpen" that was previously in operation, was dedicated to "the of child pornography and the discussion of matters pertinent to the sexual abuse of advertisement and distribution children including the safety and security of individuals who seek to sexually exploit children online." After the FBI identified the web sites Tor specific URL, they moved to seize the computer hosting the site. With the damage this can do to a child at a young age, there should be protection in place for the children on the Internet or those who have become victim to online distributed child pornography.

External Resources:

Staten Island Child Pornography Arrest
Convention on Cybercrime
UNICEF A Global Agenda for Children's Rights in the Digital Divide
UNICEF Report – The Evolving Capacities of the Child

13. RIGHTS OF PEOPLE WITH DISABILITIES & THE INTERNET

With the invention and transformation of technology and the Internet comes increasing inclusiveness that allows everyone to have access to information. People with disabilities represent the largest minority group in the world. As more education, employment, communication, entertainment, civic-participation, and government functions move primarily or exclusively online, the levels of inaccessibility on the Web threaten to make people with disabilities into second-class citizens of the information society. People of differing abilities obviously face different challenges in accessing the Internet. Principle 13 in the Charter of Human Rights and Principles for the Internet states the two major difficulties that people with disabilities face:

1. Access to the Internet

2. Availability and affordability of the Internet

There are several challenges that people with disabilities face while using or accessing the Internet. People with visual impairments can face challenges in the lack of compatibility of Web content with screen readers. For people with motor impairments, such as limited or no use of fingers or hands, the barriers are created by cluttered layout, buttons and links that are too small, and other important navigability considerations that can render entire sites and functions unusable. For persons with hearing impairments, the lack of textual equivalents of audio content can shut off large portions of the content of a site, making interactive text-chat impossible. One more issue is that people with mental disabilities may not be able to navigate complex, complicated site layouts

The Web Accessibility Initiative (WAI) has one main goal of creating an Internet that is "fundamentally designed to work for all people". Universal accessibility includes tools such as alternative text for images that gives text in place of visual images. This allows for the blind and people who don't have access to large bandwidth to see the information. Keyboard input is another tool that will aid older users who are unable to use a mouse. All global citizens should have the right to access information online whether they are physically, mentally, or socially impaired.

External Resources:

Web Accessibility Initiative
Internet use by persons with disabilities
Model ICT Accessibility Policy Report

14. RIGHT TO WORK & THE INTERNET

There are many elements in modern world that came along since the introduction of Internet to the public, and one of the main elements is being able to work remotely. The acknowledgment of such fact is extremely important, for nowadays there is a distinct relationship between work and the Internet. Thus, it is essential to know the rights that protect and endorse this relationship.

The processes of remote working is also called telecommuting, and there had been a notable trend in telecommuting for the past years according to the statistics from GALLUP, an American researched-based, global performance, management consulting company. In 1995, the percentage of telecommuters in US used to be 9%. Since then, the amount of people working remotely has been steadily increasing. According to the New Jersey Institute of Technology, 45% of people today telecommute to work. Moreover, it has to be noted that telecommuters' productivity is not affected by not being present at the office. Although remote work is still considered to be an exception, 9% of workers telecommute at least 10 workdays in a typical month. So, for those whose future will be dependent on telework, they can be assured that there are certain rights designated to protect them.

These rights outlined in the Charter are:

1. Respect for workers' rights

2. Right to access the Internet at the workplace

3. Right to work and seek employment using the Internet

A workplace should respect the fact that their employees have the right to freedom when it comes to using the internet to express their interest and form groups based on common ideologies or beliefs. Any restrictions for Internet usage by the company should be explicitly outlined and stated by the company and be readily available to the employee to access. Finally, every global citizen should have access and the right to use the Internet to find employment and to work, and they should not be punished for this right.

External Resources:

Gallup Report on Telecommuting in the U.S.

15. RIGHT TO ONLINE PARTICIPATION IN PUBLIC AFFAIRS

This principle states, “everyone has the right to take part in the government of his [or her] country, directly or through freely chosen representatives”.

One of the most crucial aspects of the Internet is that anyone can participate in decision making, regardless of their physical location. Therefore, this enables a greater amount of people that are able to participate in public affairs and take part in one’s country’s government. This includes:

1. Right to equal access to electronic services

This means that everyone has the right of having equal access to public service in the country, and more specifically everyone has the right to equal access to the electronic services in his/her country. This could include access to electronic voting or electronic broadcasts of government events.

2. Right to participate in electronic government

This simply means that wherever electronic government is available, such as online discussions or organizations, everyone must have the right to participate. Many people today are unable to participate in certain public affairs due to the fact that it requires them to be in a certain location, which may not be feasible for people without transportation or who live in a rural area. However, electronic governments level this playing field so that everyone has the right and ability to participate.

External Resources:

UN Global E-Government Survey
White House Digital Government Survey
EU eParticipation

16. RIGHT TO CONSUMER PROTECTION ON THE INTERNET

All the information that people put on the Internet is personal and private. As the cyber world grows more and more individuals and companies are trying to grab people's data for personal gains. This issue will only continue as daily tasks are conducted exclusively on the Internet

One major problem that needs to be tackled is the growing number of personal information breaches stemming from debit/credit card use. The research company Populous, conducted a survey indicating that 1 and 10 British adults were subjected to fraud on the Internet and in turn had replace their cards. These breaches span from big Multinational Corporation's to family owned businesses. In order to protect against these infringements, The National Institute of Standards and Technology suggests that, "it is extremely important to build in non-reputability which means that the identity of both the sender and the receiver can be attested to by a trusted third party who holds the identity certificates." Whatever is done, the Internet Governance Forum believes that it is consumers rights to have a safe and reliable way to shop on an online interface. It is also essential that the companies are transparent when there is a data breach. Consumers have the right to know when their personal information might have been sacrificed.

Another principle associated with consumer protection is the right to free advertisement. Companies such as Facebook, Twitter and Google are collecting personal information from customers. They utilize the personal information to generate users ads and other content. The Forum indicates that there must be proper notification from companies to individuals regarding information collection. In particular, The Internet Rights and Principles Charter says that, "Everyone has the right to exercise control over the personal data collected about them and its usage. Whoever requires personal data from persons, shall request the individual's informed consent regarding the content purposes storage location, duration and mechanisms for access, retrieval and correction of their personal data." To adopt this principle there must be laws passed in countries around the world to ensure that individual's data remains private.

External Resources:

Security of Electronic Banking
Cyber Attacks in UK

17. RIGHTS TO HEALTH AND SOCIAL SERVICES ON THE INTERNET

Health technology is changing the face of public health everyday with new tools for data collection and the use of patient data. Society has established that clinicians have moral and or legal obligations to access patient data and report certain injuries, events, and errors. As a clinician it's part of the norm to have access to patient data, however, where do we draw the line on the protection of patient data and access control? One can see this is an issue that has been debated for decades. Currently, we are living in the time of the Internet of Things where people can access a variety of resources through the Internet. With healthcare being one of the most difficult resources to afford. Providing free services through the Internet is the new solution. When it comes to information technologies, collecting patient data many argue that it might be blameworthy to not use a technological tool if there were a reason to believe that tool can improve patient care.

eHealth is an example of the future of health and social services on the Internet. eHealth responds to the needs of countries at every level of development. It helps them adapt and employ the latest information communication technologies in health. This assists policy makers determine where their country wants to go with health. eHealth is already being used throughout the world such as Spain and Africa. In each of these countries eHealth plays a different role. For example in India it was used to develop mobile services to address some of the highest rates of maternal neonatal and infant mortality. Families complete an interactive voice response-training course conducted by community health workers.

One major concern that needs to be noted in regards to the rise of eHealth is patient privacy. It is essential to protect individual's personal health information that is stored online. In Canada a letter written by the head of the Ontario Medical Association said, "We are particularly concerned to read in media reports that the government may be seeking to monetize this data-gathering ability for profit." The eHealth industry could come crashing down if data collection mechanisms are not secure and reliable.

External Resources:

National eHealth strategy toolkit
Global Observatory for eHealth series (WHO)
Compendium of innovative health technologies for low-resource settings
Patient privacy

18. RIGHT TO LEGAL REMEDY & FAIR TRIAL FOR ACTIONS INVOLVING THE INTERNET

Right to Legal Remedy & Fair Trial for Actions Involving the Internet is a big part of technology today. There is a lot that goes into actions that involve the Internet, such as Rights to a Legal Remedy, Right to a Fair trial, and Rights to due process.

Right to a Legal Remedy means that "everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him [or her] by the constitution or by law." Without Legal Remedy, no one would be able to have his or her own rights granted by the constitution.

Right to a Fair trial is defined as "everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his [or her] rights and obligations and of any criminal charge against him [or her]. The Right to a Fair trial leads to criminal trials, which follow fair trial standards. However, It is common for the right to a fair trial and to an effective remedy to be violated in the Internet Environment. For example, in 2016 China forced ITunes and movie online services to cease operations in China. That is completely against the right to a fair trial principle.

The Right to Due Process means that, "everyone has the right to due process in relation to any legal claims or possible violations of the law regarding the Internet." This right means that all states must respect all legal rights that are owned to a person. For example, when a government harms a person without following the exact course of law, this constitutes a due process violation, which offends the rule of law.

Although every individual is entitled to these rights, different countries have different legal systems. It is going to be very difficult to ensure that each person receives the same treatment and fairness regarding individuals' activity on the Internet.

External Resources:

iTunes shutdown in China
Internet: case law of the European Court of Human Rights

19. RIGHT TO APPROPRIATE SOCIAL AND INTERNATIONAL ORDER FOR THE INTERNET

For the first time in history, there is a platform available for users to find and share information in seconds. The Internet has changed the world, and it will only make progress over time. By 2020, the next billion users will have Internet access, and as of right now we do not have the capability for that much information transfers. As of right now, there are various governmental and non-governmental organizations operating in countries all around the world. These organizations such as Internet Corporation for Assigned Names and Numbers (ICANN) and Office of Science Technology Policy (OSTP), have the power to make changes and advancements to direct regulations where they have control.

In order to ensure equal user opportunity, all sites and platforms operating on the Internet need to have standards for accessible use by these marginalized groups. Individuals with disabilities make up the largest portion of marginalized groups, and they require tools such as screen readers to read any and all content on pages for visually impaired individuals. Unfortunately, due to differences in coding options, not all of these websites are compatible with screen reading software. For individuals with language barriers, it might be difficult to understand contents not available in their own language. Developing countries will be the majority of new users in the next several years and giving them Internet access is virtually useless if they cannot comprehend and learn the information.

The Internet Governance Forum (IGF) is an annual meeting of various stakeholders where public policy issues on the Internet are addressed and discussed. While there is no negotiated outcome, the IGF informs and inspires those with policymaking power in both public and private sectors to make necessary changes for everyone to advance. Unfortunately, the IGF is very under-recognized, especially by the millennial generation. It is necessary that all stakeholder opinions are heard and recognized on these issues if the society wants to reshape the Internet that people will be using for the rest of lives. This study guide was created with a purpose to raise awareness on issues at hand with the current governance of the Internet.

External Resources:

History of Internet Governance

20. DUTIES AND RESPONSIBILITIES ON THE INTERNET

The Internet is not operated by one organization or governing body, it is an amalgamation of public, private, and civil society organizations that work together to administers what users experience as the "Internet". It is upon these organizations to uphold the principles laid out in the *Charter of Human Rights and Principles for the Internet.*

As stated previously, the Internet is an amalgam of the people that use it. Essentially is a common ground for social interaction across socioeconomic or political boundaries. As such it must maintain its neutral point between the corporations, the politicians, the people, and every other community that may access the Internet. Herein lies the duty and responsibility of the users to maintain this neutrality, and to protect the freedom of expression regardless of border or status.

A prominent example of this is the transition of oversight of the Internet Assigned Numbers Authority from the National Telecommunication and Information Administration, in the U.S. Department of Commerce, to a multi-stakeholder model of governance. This process is still ongoing and has sparked considerable debate as to how to ensure the accountability of both the IANA and ICANN once it is no longer done through the U.S. Government.

External Resources:

ICANN Stewardship & Accountability
IANA Stewardship Transition Coordination Group (ICG)

NOTABLE LEGAL CASES

Elonis v. US, 135 S. Ct. 2001, 575 U.S., 192 L. Ed. 2d 1 (2015).
In the *Elonis v. US*, Anthony Elonis was arrested in 2008 and charged with five counts of violating a federal anti-threat statue. Federal law makes it a crime to transmit in interstate commerce "any communication containing any threat to injure the person of another." 18 U. S. C. §875(c). Specifically he was charged with threatening his ex-wife, co-workers, a kindergarten class, the local police, and an F.B.I agent. Elonis had posted statements on Facebook that appeared threatening to the people in his life. Prior to the posts on Facebook Elonis wife had left him and he lost his job at an amusement park. During his trial Elonis asked the court to dismiss his charges because his comments on Facebook were not true threats. He argued that he was an aspiring rap artist and that his postings on social media were merely a form of artistic expression and a therapeutic release to help get through the events that were going on in his life. Even though his ex-wife, an F.B.I agent, and others viewing his comments perceived them as threatening. Elonis still argued that he could not be convicted of making a threat because he did not intend to threaten anyone with his postings. The court denied his motion to dismiss the case and Elonis was indicted for making those threats. Following his indictment Elonis requested a jury instruction that the "government must prove he intended to communicate a true threat"[1]. This case was the foundation to determining true threats and the limits of speech on social media.

Google Spain, Google Inc., v Agencia Española de Protección de Datos (AEPD), Mario Costeja González Judgment, Case C 131/12, 13 May 2014

In 2010, the influential *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* case brought the R2bF before the Court of Justice for the European Union (CJEU) for the first time[2]. Mr. Costeja had requested Google Spain remove links directing to a newspaper article detailing past financial troubles, which Mr. Costeja claimed were damaging to his reputation as the information was no longer relevant[3]. The case was initially brought before the Spanish High Court, which then referred it to the CJEU. The CJEU sided in favor of Mr. Costeja and the AEPD, ruling that Google, as a data controller, must comply with the AEPD request to remove the links provided by Mr. Costeja. The ruling included a requirement that all Internet search engines, operating in the EU, provide a process for EU citizens to request the removal of links that direct to personal information. The CJEU ruling places responsibility of assessing whether the requested link for removal is covered under the guidelines of the ruling to the Internet search engine[4].

[1] Elonis v. US, 135 S. Ct. 2001, 575 U.S., 192 L. Ed. 2d 1 (2015).

[2] Court of Justice of the European Union. (2014) Press Release No 70/14 – Judgment in Case C-131/12. 13 May 2014 Retrieved from http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf

[3] Ibid.

[4] Ibid.

Maximillian Schrems v. Data Protection Commissioner

Maximillian Schrems v. Data Protection Commissioner may eventually shape international regulations over access to, and ownership of, online information. Maximillian Schrems an Austrian citizen has had an account with Facebook since 2008 and he filed a complaint about what was happening with all of his personal records. He eventually recovered 1,222 pages of material from a U.S company based in Dublin (Maximillian Schrems vs. Data Commissioner). As in the case of other users residing in Europe, most of the data provided to Facebook is transferred from Facebook's Ireland subsidiary to servers located in the U.S where that data is processed. Schrems launched a complaint against Ireland's supervisory authority (Data Protection Commissioner) stating that based on the information released by Snowden the law and practice of the United States does not have sufficient practices that protect against the surveillance by public authorities of the data transferred to the U.S. This case has led to the European Court of Justice declaring the U.S Safe Harbour decision is invalid. The Safe Harbour decision denies "the national supervisory authorities their powers where a person calls into question whether the decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals" (Maximillian Schrems vs. Data Commissioner) Since the Schrems case the European Parliament approved new rules fit for the digital era regarding data protection. New EU data protection rules goal is to give citizens back control of their personal data and create strong high-level data protection across Europe.

Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 578 U.S., 194 L. Ed. 2d 635 (2016).

In the U.S. Supreme Court case *Spokeo, INC. v. Robins* the concern about privacy laws that protect American consumers and the practices of online data providers are represented in this case. Thomas Robbins a Virginia man who sued Spokeo a Pasadena-based tech company that is known as a "people search engine" for releasing false data information about who he really was. Spokeo sells profiles for people drawn from data available online. When Robins searched himself he saw that he was married with children, in his 50's with a graduate degree and a professional job and none of that was true. He was actually twenty-nine, unmarried, and unemployed[5]. The suit was based on the federal Fair Credit Reporting Act of 1970. Congress passed the law after a number of people being denied mortgages or insurance because of false information on their credit card files[6]. Although Robin lost the case because he could not prove that he been harmed or damaged by the information, this case has emphasized the importance of the right to privacy on personal data.

[5] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 578 U.S., 194 L. Ed. 2d 635 (2016).

[6] Ibid

US v. Lori Drew, 2009 U.S. Dist. L.E.X.I.S. 85780 (2009).

US v. Lori Drew was the United States's first cyber bullying verdict, where Lori Drew was convicted of computer fraud for creating a fake MySpace account to trick a teenager who later committed suicide. Her charges were bought down to misdemeanors from felonies and no sentencing took place. Drew created a fake account as a young teenage boy and conducted weeks of online courtship with Megan Meier, 13, who had a history of depression. During this time the Computer Fraud and Abuse Act passed in 1986 and amended several times was expanding with the growth of technology and social media[7]. However, prosecutions under the act have only involved people who have hacked computer systems. This case was a stepping-stone to the expansion of this act and the enforcement of the Internet rights and principles to protect the public from computer crime.

US v. Morris, 928 F.2d 504 (2d Cir. 1991).

US v. Morris was the first case that introduced the importance of security on the Internet. In 1988 Morris developed a computer program known as the Internet worm. The goal of the program was not malicious harm but instead to show the lack of current security measures on computer networks. Morris designed the program to spread across a national network of computers. When Morris released the program he realized that it was replicating and re-infecting machines at a faster pace. Computers that were infected from Morris worm included: leading universities, medical research facilities, and military sites. Morris was found guilty on violation 18 U.S.C. § 1030(a)(5)(C). Section 18 U.S.C. § 1030(a)(5)(C) penalizes the conduct of an individual who "intentionally" access a protected computer without authorization[8].Morris argued that there was insufficient evidence to convict him of unauthorized access. However, the evidence permitted to the jury showed that Morris's use of the mail and directory feature constituted access without authorization. This was a very controversial case because it was not clear that Morris had actually violated the Computer Fraud and Abuse Act, simply because he was authorized to use two programs that served as loopholes his own program exploited.

[7] US v. Lori Drew, 2009 U.S. Dist. L.E.X.I.S. 85780 (2009).

[8] US v. Morris, 928 F.2d 504 (2d Cir. 1991).

REFERENCES

(n.d.). Retrieved 2015, from Europe Versus Facebook: http://www.europe-v-facebook.org/EN/en.html

(n.d.). Retrieved 2015, from Open Source Initiative: https://opensource.org/

2015 Data Breach Investigations Report. (2015). Retrieved 2015, from Verizon Enterprise: http://www.verizonenterprise.com/DBIR/2015/

Almstrom, H., & Liddcoat, J. *The Rights to Freedom of Peaceful Assembly and Association and the Internet.* Assocation for Progressive Communication.

Arifoglu, A. G., & Er, E. (2012). An Analysis of Public Internet Access Points (PIAPs). *The Journal of Community Informatics , 9* (1).

Broadband Commission . (2013). *Doubling Digital Opportunities: Enhancing the Inclusion of Women & Girls in the Information Society.* Broadband Commission (ITU, UNESCO).

(2014). *Compendium of innovative health technologies for low-resource settings (2011-13).* World Health Organization. World Health Organization.

Convention on Cybercrime. (2001, Nov 23). Budapest.

Council of Europe. (n.d.). *Internet content and equality between men and women*. Retrieved 2015, from Council of Europe: http://www.coe.int/en/web/portal/internet-and-equality

Creative Commons. (n.d.). Retrieved 2015, from https://creativecommons.org/

Cybercrime, C. o. (2001). Convention on Cybercrime. *Council of Europe Treaty No.185* .

Dewey, C. (2014, October 14). The only guide to Gamergate you will ever need to read. *The Washington Post* .

Digital Government: Building a 21st Century Platform to Better Serve the American People. (n.d.). Retrieved 2015, from WhiteHouse.org: https://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html

DLA Piper. (n.d.). *Data Protection Laws of the World.* Retrieved 2015, from DLA Piper Data Protection: http://www.dlapiperdataprotection.com/#handbook/world-map-section

Electronic Frontier Foundation. (2015). *Deeplinks Blog*. Retrieved from Electronic Frontier Foundation: https://www.eff.org/deeplinks

eParticipation. (2015, Mar` 17). Retrieved 2015, from European Commission: https://ec.europa.eu/digital-agenda/en/eparticipation

European Commission. (2015, Mar 11). *National data protection authorities*. Retrieved from European Commission: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

European Commission. (2015, 10 27). *Net Neutrality*. Retrieved from Digital Agenda for Europe: https://ec.europa.eu/digital-agenda/en/net-neutrality

European Court of Human Rights. (2011). *Internet: case law of the European Court of Human Rights.* European Court of Human Rights, Division of Research. Council of Europe.

(2014). *Factsheet on the "Right to be Forgotten" ruling (C-131/12).* European Commission. European Commission.

Federal Communications Commission. (n.d.). *Open Internet* . Retrieved 2015, from FCC: https://www.fcc.gov/general/open-internet

Galperin, H., Mariscal, J., & Barrantes, R. (2014). *The Internet and Poverty: Opening the Black Box.* Diálogo Regional sobre Sociedad de la Infomación (DISRSi); International Development Research Centre (IDRC).

GitHub. (n.d.). Retrieved 2015, from https://github.com/

(2013). *Global Action on Cybercrime (GLACY).* European Union and Council of Europe.

Global Observatory for eHealth. (n.d.). Retrieved from World Health Organization: http://www.who.int/goe/publications/ehealth_series_vol1/en/

Gonzalez, A. L. (2015). Disadvantaged Minorities' Use of the Internet to Expand Their Social Networks. *Communication Research* .

Greenpeace International. (2012, 2012 17). *Greenpeace International*. Retrieved from How Clean is Your Cloud?: http://www.greenpeace.org/international/en/publications/Campaign-reports/Climate-Reports/How-Clean-is-Your-Cloud/

Helland, C. (2005). Online Religion As Lived Religion. *Heidelberg Journal of Religions on the Internet , 1.1*.

History of Internet Governance. (n.d.). Retrieved 2015, from Internet Society: http://www.internetsociety.org/history-internet-governance

IANA Stewardship & Accountability. (n.d.). Retrieved 2015, from ICANN: https://www.icann.org/stewardship-accountability

Internet Domain Name Expansion Now Underway. (2013, Oct 23). Retrieved from ICANN: https://www.icann.org/resources/press-material/release-2013-10-23-en

Internet Governance Forum. (n.d.). Retrieved 2015, from http://www.intgovforum.org/cms/

Internet Governance Forum (IGF). (n.d.). Retrieved 2015, from YouTube: https://www.youtube.com/user/igf

Internet use by persons with disabilities: Moving forwards. Internet Society.

Internet.org. (n.d.). Retrieved 2015, from Internet.org: https://info.internet.org/en/

Jones, J. M. (2015, Aug 19). *In U.S., Telecommuting for Work Climbs to 37%.* Retrieved 2015, from Gallup: http://www.gallup.com/poll/184649/telecommuting-work-climbs.aspx

Lansdown, G. (2005). *The Evolving Capacities of the Child.* Save the Children; UNICEF.

Levine, M. (2013, May 28). *Controversial, Harmful and Hateful Speech on Facebook.* Retrieved from Facebook: https://www.facebook.com/notes/facebook-safety/controversial-harmful-and-hateful-speech-on-facebook/574430655911054

Livingstone, S., & Bulger, M. E. (2013). *A Global Agenda for Children's Rights in the Digital Age: Recommendations for Developing UNICEF's Research Strategy.* London School of Economics and Political Science; UNICEF Office of Research.

(2014). *Model ICT accessibility: Policy Report.* ITU; Global Initiative for Inclusive ICTs.

(2012). *National eHealth Strategy Toolkit.* World Health Organization, ITU.

OECD. (2015). Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document.

Open Net Initiative. (2015). Retrieved from Open Net Initiative : https://opennet.net/about-oni

Overview. (n.d.). Retrieved 2015, from IANA Stewardship Transition Coordination Group (ICG): https://www.ianacg.org/

Overview: the TRIPS Agreement. (n.d.). Retrieved 2015, from World Trade Organization: https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm

Report on encryption, anonymity, and the human rights framework. United Nations Human Rights, Office of the High Commissioner. United Nations.

Reporters Without Borders. (2015). Retrieved from Reporters Without Borders: http://en.rsf.org/internet.html

Teaching Copyright. (n.d.). Retrieved 2015, from teachingcopyright.org

U.S. Department of Commerce. (2015, Oct 9). *Advisory notice on the invalidation of the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks.* Retrieved from Export.gov: http://www.export.gov/safeharbor/index.asp

UN E-Government Survey 2014. (2014). Retrieved 2015, from UNPAC: https://publicadministration.un.org/egovkb/Reports/UN-E-Government-Survey-2014

Weber, R. H. (2014). Internet of Things - New security and privacy challenges. *Computer Law and Security Review* , 23-30.

Wikipedia. (n.d.). *Internet censorship and surveillance by country*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Internet_censorship_and_surveillance_by_country

Wikipedia:About. (n.d.). Retrieved 2015, from Wikipedia: https://en.wikipedia.org/wiki/Wikipedia:About

York, J. (2014, Mar 20). *Why is Turkey Blocking Twitter?* Retrieved from Electronic Frontier Foundation: https://www.eff.org/deeplinks/2014/03/why-turkey-blocking-twitter

`