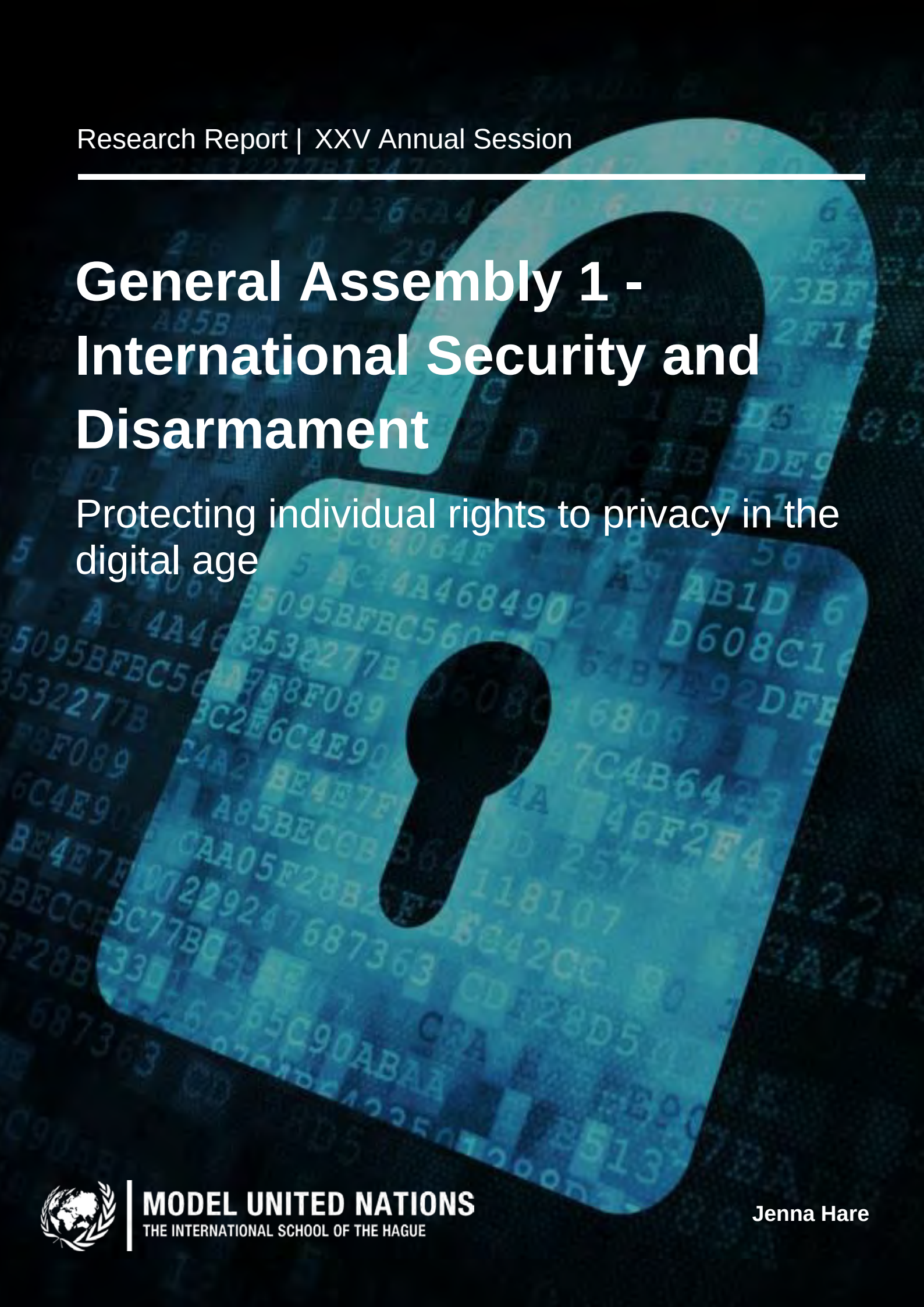


Research Report | XXV Annual Session

General Assembly 1 - International Security and Disarmament

Protecting individual rights to privacy in the digital age

MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Jenna Hare

Forum: General Assembly 1 - International Security and Disarmament

Issue: Protecting individual rights to privacy in the digital age

Student Officer: Jenna Hare

Position: Deputy Chair

Introduction

In this digital era, there has been a significant increase in the use of technology. Advances are being made to invent and discover more sophisticated technology every day. The increase in people using digital media is being driven by the easy accessibility and quick responses. “92% of Internet users” report that they use the Internet to ‘send or read e-mails’, showing that the Internet is commonly used for personal communication purposes. It addition, personal information, such as on Google, Facebook or Microsoft, can become vulnerable on the Internet.

Edward Snowden, for example, was able to leak information from the National Security Agency (NSA) to the media in 2013. This event was only the start of a large number of scandals where citizens found out the government had taken unauthorized information from them, which shocked the world. Seeing as the human race is continuing to advance and develop technology, we are facing the problem of how to keep individual rights to privacy intact.

Definition of Key Terms

The Digital Age

This time period refers to the late 1970’s up until the present time, where increasingly advancing technology is being introduced. This allows us to store and transfer information quickly and freely on a digital media.

The Right to Privacy

Defined by the Universal Declaration of Human Rights (UDHR) as, “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, or correspondence, or to unlawful attacks on his honor and reputation.” (As shown in more detail in Appendix II)

Surveillance

Refers to the attentive and continuous observation or watch over a place/person/group. The watch is usually over someone who is a suspect, for example in a prison.

Correspondence

In the context of this issue, correspondence refers to communication, such as letters. In the digital age however, the correspondence is frequently through e-mails or digital media.

Cookies

A web cookie is a small piece of data that contains information about online users. It is sent from a site and stored into the user’s web browser and used on the web page without their consent.

Whistleblower

This term refers to a person who turns another in for illegal activity or an act of wrongdoing, whether it be informing a single other or making a public announcement.

Internet Censorship

“The control or suppression of what can be accessed, published, or viewed on the Internet. It may be carried out by governments or by private organizations at the behest of government, regulators, or on their own initiative.”

General Overview

Due to the statement by the UDHR, no personal information on the digital media should be violated. The debate is whether fellow citizens or the national government should have access to your correspondence and personal information.

Edward Snowden and the NSA

The NSA is an agency, which aims to protect all US national security systems and oversee foreign information. In June 2013 private information from the NSA was leaked to the public through Edward Snowden, a computer professional. This grabbed international attention as he gave thousands of classified documents to journalists and publishers. His act has received a mix of emotions, as he has been called both a whistleblower and a traitor. Many call him a whistleblower as the information which he discovered included that the NSA was gathering "millions of email and instant messaging contact lists, searching email content, tracking and mapping the location of cell phones… …and that the agency was using cookies to "piggyback" on the same tools used by internet advertisers "to pinpoint target for government hacking and to bolster surveillance." In this sense, it left the public outraged that the government was compromising their information. On the other hand, Robert Gates, the former Defense Secretary, called him a traitor for not working inside of the carefully, thought-out system. He stated that he thinks, "that the revelations have done a lot of damage."

Furthermore, it was discovered that the US National Security Agency (NSA) used PRISM, a data collection program, which could recall stored telecommunication data that matched specific search terms. This led the NSA to target such communications. It did not only target citizens of the US, but also those in the Bahamas. This shows that this, what at first looks like a national problem, is in fact international. The NSA surveillance was linked in to the Bahamian government without knowledge or consent. It can now recall and store all telecommunication audio clips and can play them for up to a month. This system is part of a bigger called MYSTIC, and is now branching out in to countries such as Mexico, The Philippines and Kenya.

The Surveillance Industry

In the expanding surveillance industry, it is common to spy on citizens. "American, British and Allied intelligence agencies are soon to embark on a massive, billion-dollar expansion of their global electronic surveillance system." This will allow the agencies to monitor current communications between citizens, and possibly intercept them. A strong barrier of high technology protects such agencies, and there are currently no measures taken against them. An example of this is Project 415, a top-secret surveillance system. It hacks into billions of calls per year in the United Kingdom (UK) alone. They rely on international satellite signals to locate and target individuals. Due to their success, it has lead to teams inside of the project to train other computer centers on how to carry out international interceptions, spreading the skills of hacking worldwide, with no control.

Blocking U.S Spies

There is already attempt of preventing U.S spies from hacking in to telecommunication in the Russian Federation. Current Russian President, Vladmir Putin, “signed a law ... that obliges Internet companies to store Russian citizens' personal data inside the country.” This law is changing the rules of processing personal data and information in the digital era. Any operators of personal data will need to keep this inside of Russia, by using home databases; a more in-depth description of the law can be seen in Appendix IV. Yevgeny Fedorov, a Russian politician, stated, "that's where the censorship and revision of the events taking place in Russia come from,... All the information is stored there and used against Russia. To avoid this and protect the country, we have to take these objects under national control.” Their main goal is to prevent US spies from hacking in to the country's telecommunication networks.

This will have a large impact on social networking sites, as they will need to alter their systems to be able to function in Russia. It will be difficult to transmit international communications through the Internet. Instead, own social networking sites such as Russia’s ‘Vkontakte’ will benefit from this change, and hopefully secure citizen’s private personal information.

Public Awareness

The scandals about governments taking unauthorized information from its citizens lead to general awareness about rights to privacy. It lost peoples trust with their nation’s government, and therefore the public continues to want more transparency on this issue. Furthermore, it led people to believe that their private information could not be trusted on the digital media anymore. Despite the increase in modern technology it is feared that it will not be used widely enough due to lack of trust with private information, which also prevents true freedom of expression. The acts of the Government contrasted what is stated in the European Convention of Human Rights (see Appendix I).

Internet Censorship

Internet censorship has been apparent in the recent years, and is usually carried out through national governments. Most countries have moderate Internet censorships, however some are more severe than others. Some governments decide to block sites, limiting access to news broadcasts, for example, or place restrictions on internet users because of social, religious and commonly, political reasons.

Anticipated Events

Internet censorships may also occur because of anticipation of certain events such as protests or riots. An example of this is Arab Spring, which started in Tunisia in 2010 before spreading to other Arab countries. It happened at the time that many protests broke out. The government shut down some social media sites, as they feared that their citizens were communicating and spreading ideas between countries, online.

More events such as these have occurred, such as the fact that Twitter was blocked in Egypt in late January of 2011 when major Egyptian protests broke out. This happened in the United Kingdom too, when in 2011, current Prime Minister, David Cameron, threated to shut down Twitter due to riots. However, no actions were eventually taken in the United Kingdom.

Internet Censorship in China

A prime example of extreme Internet censorship is in China. They have the license to shut down sites through the *Public Pledge on Self-Discipline for the Chinese Internet.* Not only does the government block sites, such as *Facebook* at *Twitter* in 2009, but they also monitor individual's uses of the Internet. They do not, however, monitor all Internet correspondence such as inside chat rooms/forums, as they do not have the time. But, with the thought that their website could be shut down, many sites hire internal staff themselves to complete this monitoring for the government. Their job is to scan chat forums, in which the citizens are unaware of, to search for inappropriate comments on the country's political status. There is, however, no information on if such staffs are seeing other private information of citizens that do not have to do with political issues.

They are known to place fines and imprisonment for 'unacceptable' uses of the internet. Unacceptable uses include communicating internationally on issues such as corruption and signing on to petitions. Amnesty International has stated that China "has the largest recorded number of imprisoned journalists and cyber-dissidents in the world".

Due to the demand of social media in China, the government released their own version of *MySpace* in April of 2007, where there is a filtering system to check for religious and political topics of conversation. There is also a chance for users to report other users for any inappropriate leaked information they come across.

'In a 2012 Internet Society survey 71% of respondents agreed that "censorship should exist in some form on the Internet". In the same survey 83% agreed that "access to the Internet should be considered a basic human right" and 86% agreed

that "freedom of expression should be guaranteed on the Internet". Despite the percentage of citizens wanting censorship, it is not clear on what. Seeing as though a high percentage feels the access to the Internet should be a human right, the restrictions shown, especially in China, are stopping freedom of expression and access to sites of their choice.

Twitter Ban

Twitter is currently blocked in North Korea, China and Iran. It was blocked in Turkey for a long time, due to the spreading of videos, which insult the country's founder, Mustafa Kemal Ataturk. The ban from the Turkish government was released 2 weeks after it was implemented, but it continued to block 2 users whom pointed out political and economic problems with the country.

Rights of our Personal Information

More of your personal information from the Internet is exploited than you think. Common examples of this are store advertisements of products you have looked at on another sites or even companies finding your credit history. In 2014, Google confirmed that e-mails by anyone who uses their services are likely to be scanned. In specific, they stated; "Our automated systems analyze your content (including e-mails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored." Their focus is to take and analyze data, to be used for advertising purposes. However, there are no boundaries on what such companies are scanning. If they are indeed able to analyze data for further features, are there any restrictions on the personal information they also have access to, and is this going against our human right of privacy?

Major Parties Involved and Their Views

United States of America (USA)

The United States of America were the central party when the Edward Snowden issue arose. They are continuously working on preventing such a national problem to rise again as it was the US citizens whose information was violated and who were highly affected by the lack of privacy in their country. Current president, Barack Obama, stated in January 2015 that a legislation were soon to be released as a plan to protect information of American's and prevent cyber-attacks in the digital age.

United Kingdom (U.K)

Hackers prominently affect the United Kingdom. They are the prime subject to Project 415, and the UK has billions of phone calls hacked every year. Furthermore, according to a poll in December 2014, “92% of internet users in Great Britain were worried about their privacy online”. Citizens of the UK are becoming aware of their status on the internet, and are willing to solve this issue. Citizens have already started deleting cookies, changing privacy settings and reading privacy policies.

European Union (EU)

There have been rules put in place by the EU that state to ensure the high protection of personal data. There has been the formation of the EU Data Protection Directive, which strives to “ensure that personal data can only be gathered under strict conditions and for legitimate purposes.” The EU are staying updated on the issue, as in 2012 they released a reform of their 1995 data protection rules, including topics such as cookies and new technologies.

People’s Republic of China

China is the major party in Internet censorship worldwide. They are known to be strict and controlled in what they are allowing their citizens to see. In 2002, The Internet Society of China, a non-governmental organization (NGO) that includes members from all over the Internet business including researchers and schools, launched the *Public Pledge of Self-Discipline* for the Chinese Internet Industry. It was set in place as an agreement between the Chinese Internet Industry and companies who operate sites in China to prevent transmission of information to do with breaking laws or suspicious threats. It has been enforced strictly, as without signing on to this agreement you may not receive an official license to post Internet content.

China is therefore constantly reviewing and analyzing citizen’s use on the internet, perhaps having access to personal information which could be seen as breaking laws of privacy.

Timeline of Events

Date	Description of event

December 10th, 1948	The Universal Declaration of Human Rights was adopted
November 4th, 1952	National Security Agency (NSA) was formed
October 24th, 1995	EU released a directive on the protection of individuals with regards to the processing of personal data and on the free movement of such data
June, 1997	The Electronic Privacy Information Center reports 17 out of the 100 most popular internet sites have privacy policies
March 16th, 2002	The Internet Society of China launched the *Public Pledge on Self-Discipline for the Chinese Internet Industry*
November 2003	The Golden Shield Project was launched
2007	Launch of the US surveillance program, PRISM
April 2007	The Chinese released original version of Myspace, where any comments on political matters are banned
Late 2009	The Chinese government blocked social media sites, Facebook and Twitter
2010	Liu Xiaobo, a Chinese human rights activist, became a forbidden topic on social media due to winning the 2010 Nobel Peace Prize
December 17th, 2010	The first of the outbreaks of protests in Tunisia, starting the 'Arab Spring'
January 25th 2012	Reform of the EU's data protection rules to strengthen online privacy rights and boost Europe's digital economy was released
June, 2013	Edward Snowden leaked classified information from the US NSA to the media
June 3, 2013	The Chinese Government banned the use of the 'candle emoji' to be places on social media comments, as it links to death
March 20, 2014	Twitter was blocked in Turkey
July, 2014	Russian President Vladimir Putin signed the new personal-data measures in to law

September, 2014	OHCHR presented their report on the Right to privacy in the Digital Age to the Human Rights Council

UN involvement, Relevant Resolutions, Treaties and Events

The UN has only become active on the issue in the past few years, as that is when most of the problems arose. The Office of the High Commissioner for Human Rights (OHCHR) looks over major programs in protecting human rights internationally. Following the concern of the UN General Assembly on this issue, they created a report on digital privacy, which was presented in September 2014 and further discussed in the resolution of the General Assembly in December 2014. Furthermore, there have been multiple panels in the Human Rights Committee on this issue. Listed below are the most relevant resolutions, treaties and events that have occurred on this issue;

- Universal Declaration of Human Rights, 10 December 1948 (**Article 12 and 19**, stated in more detail in Appendix II)
- Reform of the EU's 1995 data protection rules to strengthen online privacy rights, 25 January 2012 (**Directive 95/46/EC**)
- Developments in the field of information and telecommunications in the context of international security, 9 January 2014 (**A/RES/68/243**)
- Panel on the Right to Privacy in the Digital Age, 15 April 2014 (**A/HRC/DEC/25/117**)
- The Right to Privacy in the Digital Age, 18 December 2014 (**A/RES/69/166**)

Evaluation of Previous Attempts to Resolve the Issue

Following the resolution submitted to the General Assembly in 2014, there have been minimal attempts to resolve this issue. Firstly, the committee asked member states to review previous procedures and legislation regarding surveillance. This would mean states are ensuring that they are following the UDHR. However not all states have yet reviewed this as there are still international legislations which are not in accordance to the right of digital privacy.

The Federal Bureau of Investigation (FBI) has also been taking initiative by wanting to monitor emerging threats through social media. This is so they can quickly track and identify

them. This can then lead to the safety and wellbeing of surrounding citizens, and preventing disasters from occurring. Monitoring such threats would include creating a new web application to monitor Twitter, Facebook and news reports such as on CNN. However, there have been worries that law enforcement will come in to action, as there is a risk of freedom of speech being compromised.

Outside of the UN, other attempts have taken place such as the US forming a system called VANISH. VANISH was created through the University of Washington and its aim is to eradicate old, online correspondence that users have supposedly 'deleted', but still remain online. An assistant professor in the company stated, "We wanted to create a system that would allow our data to self-destruct and become permanently unreadable." This system is hoped to be effective, as it gives the owner the responsibility of setting a time period that they wish their correspondence to be available for. "It works by creating a secret key, which is split into small pieces and shared across many users on a peer-to-peer network. Over time, as the users join and leave the network, the pieces of the key will disappear, rendering the data unreadable." Any archived or backed-up copies will be forever unreadable, by both the system and the public.

It is difficult to analyze and evaluate the recent attempts of resolving this issue, as work that is carried out by governments and federal agents are extremely confidential, and giving this information could mean losing their ability to protect their nation.

Possible Solutions

The first obvious solution to preventing this problem from growing in the future is tackling the legislation aspect. Placing effective laws against such issues will not only raise awareness of the issue but also hopefully decrease the number of criminals. It is also important to keep such legislative bodies up to date with updates that cover recent and emerging technologies. The digital age works rapidly, and keeping frequent updates on treaties and laws is the key to individual privacy.

Another issue is individuals placing their personal data on online databases with no thought of who could see and use this content. Therefore, public awareness must be spread to allow the public to see the dangers of spreading confidential information and how they can possibly prevent this. As previously mentioned, UK citizens have already begun using methods such as changing privacy settings, reading privacy policies and deleting cookies. A more detailed list of such preventions is shown in Appendix III.

Furthermore, to prevent this issue from arising, there needs to be stronger and more effective penalties towards the persons who have already gained unauthorized access to another's private information and either receive, process or use it. Edward Snowden was given a maximum of 30-year prison sentence from the US government; however, many believe that he should be behind bars for his lifetime. There is currently no updated legislation for punishments on crimes such as those occurring in the digital age.

There is also little recognition towards whistleblowers. Whistleblowers bring attention to large cooperation's that abuse their power, and therefore some believe they should be congratulated. This could include, for example, giving them protection or economic help, in thanks for their input to society.

Bibliography

Blenford, Adam, and Christine Jeavans. "After Snowden: How Vulnerable Is the Internet?" *BBC News*. BBC, 27 Jan. 2014. Web. 13 June 2015. <http://www.bbc.co.uk/news/technology-25832341>.

Campbell, Duncan. "Somebody's Listening." *Somebody's Listening Project 415*. N.p., 12 Aug. 1998. Web. 13 June 2015. <http://cryptome.org/jya/echelon-dc.htm>.

"Can UK Consumers Have Their Digital Privacy, Please?" *EMarketer*. N.p., 18 Feb. 2015. Web. 13 June 2015. <http://www.emarketer.com/Article/UK-Consumers-Have-Their-Digital-Privacy-Please/1012066 - sthash.ZxEd3YhU.dpuf>.

"Edward Snowden." *Wikipedia*. WikiFoundation, 12 June 2015. Web. 13 June 2015. <https://en.wikipedia.org/wiki/Edward_Snowden - Release_of_NSA_documents>.

Epatko, Larisa. "Former Defense Secretary Gates Calls NSA Leaker Snowden a 'traitor'." *PBS Newshour*. PBS, 14 Jan. 2014. Web. 13 June 2015. <http://www.pbs.org/newshour/rundown/gates-on-snowden/>.

Gillmor, Dan. "As We Sweat Government Surveillance, Companies like Google Collect Our Data." *The Guardian*. N.p., 18 Apr. 2014. Web. 1 Aug. 2015. <http://www.theguardian.com/commentisfree/2014/apr/18/corporations-google-should-not-sell-customer-data>.

"Internet Censorship." *Wikipedia*. Wikimedia Foundation, n.d. Web. 01 Aug. 2015. <https://en.wikipedia.org/wiki/Internet_censorship>

Koebler, Jason. "FBI Wants to Monitor Social Media for 'Emerging Threats'"*US News*. U.S.News & World Report, 27 Jan. 2012. Web. 13 June 2015. <http://www.usnews.com/news/articles/2012/01/27/fbi-wants-to-monitor-social-media-for-emerging-threats>.

Lee, Dave. "This Website Will Self-destruct..." *BBC News*. BBC, 12 Aug. 2009. Web. 13 June 2015. <http://news.bbc.co.uk/2/hi/technology/8197449.stm>.

Lopatnikova, Ekaterina. "Russia's Internet Privacy Act Will Have Wide Implications for Foreign Companies." *PLB News*. N.p., 16 July 2014. Web. 01 Aug. 2015. <https://www.privacylaws.com/Publications/enews/International-E-news/Dates/2014/7/Russias-Internet-Privacy-Act-will-have-wide-implications-for-foreign-companies/>.

"Most Popular Internet Activities." *Infoplease*. Infoplease, 22 July 2008. Web. 15 May 2015. <http://www.infoplease.com/ipa/A0921862.html>.

"National Security Agency." *Wikipedia*. WikiFoundation, 12 June 2015. Web. 13 June 2015. <https://en.wikipedia.org/wiki/National_Security_Agency>.

"New Russian Law Bans Citizens' Personal Data Being Held on Foreign Servers." *RT*. N.p., 5 July 2014. Web. 1 Aug. 2015. < http://www.rt.com/politics/170604-russia-personal-data-servers/>

"Obama Announces Legislation Protecting Personal Data, Student Digital Privacy." - *RT USA*. N.p., 12 Jan. 2015. Web. 13 June 2015. <http://rt.com/usa/221919-obama-privacy-student-consumer/>.

"Online Privacy." *Digital Agenda for Europe*. N.p., 18 Mar. 2015. Web. 13 June 2015. <https://ec.europa.eu/digital-agenda/en/online-privacy>.

Phillipson, Gavin. "Q&A: The Right to Privacy." *BBC*. BBC, 14 June 2013. Web. 18 May 2015. <http://www.bbc.co.uk/religion/0/22887499>.

"Public Pledge on Self-Discipline for the Chinese Internet Industry."*Wikipedia*. Wikimedia Foundation, n.d. Web. 01 Aug. 2015. <https://en.wikipedia.org/wiki/Public_Pledge_on_Self-Discipline_for_the_Chinese_Internet_Industry>.

"The right to privacy in the digital age." *SpringerReference* (2011): 3+. Office of the United Nations High Commissioner for Human Rights, 30 June 2014. Web. 13 June 2015. <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf>.

Appendices

Appendix I

Article from the European Convention on Human Rights, Article 8 which is relevant to the Right to Privacy

Article 8: Right to privacy

- (1) Everyone has the right for his private and family life, his home and his correspondence.
- (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

http://www.bbc.co.uk/religion/0/22887499

Appendix II

Articles in the Universal Declaration of Human Rights, which are relevant to privacy and freedom of expression

Article 12.

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

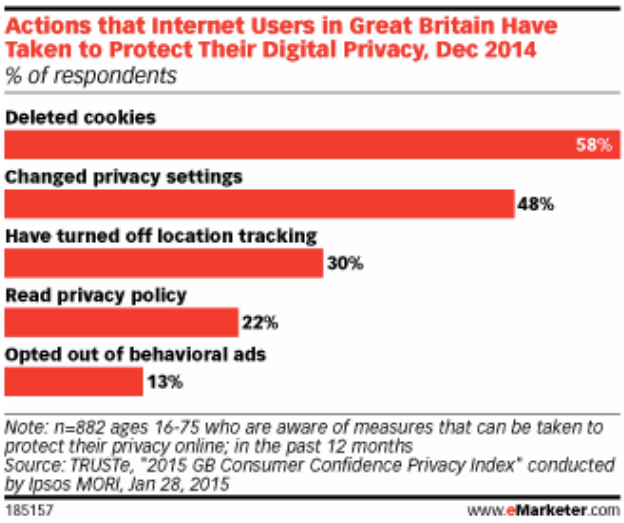
Article 19.

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

http://www.un.org/en/documents/udhr/index.shtml#a12

Appendix III

Bar chart showing actions that internet users in Great Britain have taken to protect their digital privacy



http://www.emarketer.com/articles/results.aspx?q=digital%20privacy&ecid=MX1087

Appendix IV

The new law of Russia stipulates that;

When collecting, recording and processing personal data of Russian nationals, data controllers must use servers located on the Russian territory. The only exception to this requirement concerns the cases of personal data processing for the purpose of implementation of an international agreement or related Russian law, administration of justice and enforcement of court ruling, provision of public and municipal services, mass media or creative work.

Russia's Data Protection Authority (DPA) will be able to block public Internet access to any service that does not comply with this requirement. In particular, it is assumed that a Register will be created to list those in breach of data subject's rights. This would include identifiers, such as domain names and/or indices of web pages of violators, and network addresses.

https://www.privacylaws.com/Publications/enews/International-E-news/Dates/2014/7/Russias-Internet-Privacy-Act-will-have-wide-implications-for-foreign-companies/

Appendix IV

List of Useful Sources and Links:

http://www.consumerreports.org/cro/money/consumer-protection/big-brother-is-watching/overview/index.htm

http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

http://www.un.org/en/ga/69/resolutions.shtml