Fall 2016

Violating of Individual Privacy: Moroccan Perceptions of the Ban of VoIP Services

Tyler Delhees
SIT Study Abroad

Violating of Individual Privacy:

Moroccan Perceptions of the Ban of VoIP Services

Delhees, Tyler

Belghazi, Taieb

SIT Morocco: Multiculturalism and Human Rights

4 December 2016

ABSTRACT

On January 6, 2016, the Moroccan telecommunications regulatory agency, the ANRT, announced a ban onVoice Over Internet Protocol(VoIP)calling services such as Skype, WhatsApp, and Viber. The ban triggered sweeping opposition among the Moroccan public, opening discussion of digital rights, censorship, and Internet governance. Considering liberal democratic rights in the 2011 Moroccan Constitution and a history of censorship, this study analyzes the official justification of the ANRT alongside additional explanations involving business interests and the security services. The purpose of this study is to gauge the perceptions of Moroccans on the decision of the ANRT and provide a holistic explanation. Through interviews with three professionals, this study examines alternativeperceptions of the ban and compares the bases of each.

TABLE OF CONTENTS

INTRODUCTION	3
LITERATURE REVIEW	3
METHODOGY	5
CONTEXT	6
PERSPECTIVES	15
CONCLUSION	19
ACKNOWLEDGEMENTS	21
REFERENCES	22
APPENDIX	27

INTRODUCTION

Considering the waves of anti-establishment politics around the world today, digital media and the potential vested within mustered much attention. Social media's effects on political dynamics in an age of globalization are hackneyed in scholarly work, yet the availability of new technologies is too often assumed. While cyberspace offers societies new public space and a forum for fighting injustice and violations of human rights, its ultimate potential only reaches as high as Internet governors allow. In democratic and nondemocratic countries alike, the governors have proven to be adroit in limiting the full potential of digital technologies.The Moroccan experiment with banning Voice over Internet Protocol (VoIP) services presents a case of government meddling in the cyber domain and effectively limiting the degree to which society can utilize the technology. It is this juxtaposition that this study will examine while seeking to map expert perceptions of the Moroccan regulation of VoIP and its ultimate unraveling. By analyzing and comparingexpert perceptions, this research elaborates on the Moroccan cybersecurity context and positions the ban at the intersection of human rights and new technologies.

LITERATURE REVIEW

The use of digital technologies and its socio-political effects have been amply researched. For this study, previous literature can be divided thematicallyinto that on free speech, surveillance theory, andauthoritarian reactions to digital technologies.

Discussing the limits of free speech in Moroccan society, Smith and Loudiyidentify three "red line" topics—the king and the royal house, Islam as the state religion, and territorial integrity—which have become de facto taboos in public discourse and grounds for state action

against citizens (2005). Although the regime of Mohammed VI has allowed greater freedom than the previous regime, these red lines remain fair grounds for arrests, detentions, and censorship of the media. Smith and Loudiyargue that "regulative control is exercised both through self-censorship and the manipulation of information" (2005). Conceptually, David Lyon in *The Electronic Eye* explains self-censorship as a result of state surveillance and the public fear created by it. He puts forth Jeremy Bentham's panoptic prison plan, further applied to technology by Michel Foucault, as a lens through which to understand electronic surveillance. Borrowing from Foucault, he theorizes electronic surveillance as gaining its power from the invisibility, uncertainty, and fear of punishment generated (Lyon, 1994). The effectiveness and enforcement of order is established through these means in surveillance in much the same way that it is established in the panoptic prison.

In political sciencediscourse, perceptions of the effects ofinformation and communication technologies (ICTs)vary between the digital optimists and digital pessimists (Zaid, 2016). The digital optimists emphasize the democratizing effect of ICTs and their use as a public spaceparticularly during the Arab Spring uprisings. The digital pessimists counter with three undemocratic threats posed by the same technologies: Internet openness, surveillance, and big data. On the side of the digital pessimists, Bruce Schneier argues that governments and multinational corporations control the upper handand outweigh the benefits offered by the optimists (Zaid, 2016). Elizabeth Bryant analyzes authoritarian use of ICTs and illuminates how regimes enhance their power incyberspace,a "contested space"(2012).Explaining thatgovernments will utilize technologies if available, she quotes EvgenyMorozovwho proclaimed, "technology changes over time…human nature, hardly ever" (Bryant, 2012).Moreover, Shirkyexplains the digital behavior of governments as a reaction to the

"conservative dilemma," a threat to authoritarianism from the public awareness that new technologies create (2011). This public awareness is an element that contributes to the expansion of the cyber public sphere.

METHODOLOGY

Research design

This study is designed to explore expert opinion on the topics of the ANRT's ban and digital rights in Morocco through purposeful sampling. Data is compiled from academic and professional sources as well as semi-structured interviews with expertsin the ICT field. In order to focus on expert opinion, interviews with the Moroccan public are excluded from this study. Interviews were conducted with a digital rights activist, an IT consultant, and a software developer. Each was conducted between November 12 and December 3, 2016 and voice-recorded for review. The semi-structured approach to interviews benefited this research as each individual was encouraged to speak according to his specific specialties. English and Arabic were the languages used during this study; interviews in Arabic were interpreted with the aid of a translator.

Limitations

Moreover, this study is limited by personal bias, the length of study, and language. First, my status as a foreign student with a temporary itinerary in Morocco contributed to the difficulty of contacting individuals and conducting candid research. This knowledge and recognition of my American identity contributed to the information obtained as well as the limited access to professionals. Second, this study was limited by its timeline. Individuals were contacted by

means of phone calls, e-mail, and Twitter, yet establishing contact and scheduling interviews was difficult within the timeframe of three weeks.Even so, I established contact and rapport with individuals who had been introduced to me through my advisor and academic director.Finally, I must also account for the limited use of French in this study. Not attaining a working proficiency in the language limited the technical articles from which I could research.

Bias

As an American student biased towards liberal democratic principles, my perspective is biased to frame the ANRT ban as an issue of privacy and national security. This debate in the United States and the revelations of Edward Snowden influenced my approach to this topic. Further, my position as a foreigner in Morocco affects the quality of cross-cultural consideration in this study. Recognizing the limits of this research and how my background affects it, I have attempted to present a candid and coherent account of this recent development.

CONTEXT

The ban and its lifting

The ANRT officially enforced a ban on VoIP services on January 6, 2016. However, implementation of the ban was gradual and unannounced months before the official ANRT announcement. Although VoIP services had previously been stopped without announcement in 2014, Moroccans noticed that services began stopping prior to the ban. HananeBoujemi, a technology policy expert with experience in the MENA region, mentions that the baninvokes a 2004 resolution from the ANRT seeking to protect the financial interests of telecom operators. While Boujemi does not have specific economic figures relevant to the ban, she notes that the

ban had hurt customer choice and the image of the telecoms (2016). Further, it is important to recognize that the ANRT, not the telecom operators, had the final word. In fact, both INWI and Meditelexpressed frustration with the ban and its effects on their images as many blamed the operators (INWI Withdraws from Maroc Web Awards After ANRT Banned Skype, FaceTime, 2016).

After ten months of enforcing the ban through telecom operators, the agency officially restored VoIP services on November 4, 2016. Like the beginning of the ban, reports of the ending of the ban surfaced before the ANRT communiqué. The ending was suspiciously preceded by the removal of the director general of the ANRT, Azeddine El MountassirBillah, which will be discussed in perspectives section. Two factors appear to explain the ultimate decision of the agency to lift the ban. First, COP22 meetings were held just a week later and the accompanying international spotlight likely put pressure on the state to modify the ban. Second, a Brookings report on Internet shutdowns estimated that the ANRT ban had contributed to a $320 million loss in the Moroccan economy(West, 2016). Most media outlets disseminated news of the report, and popular protests sprung up thereafter (MarouaneHarmach, personal communication, November 18, 2016). The ANRT officially described its decision in a statement saying, “The decision (to lift the ban) comes after the ANRT’s evaluation of the telecom national and international markets, the legal context and taking into consideration the requirements to develop a sector that benefits customers” (You Can Make Skype Calls in Morocco Again). The agency retreated from its original legal invocation.

2011 Constitution, the Judicial System, and Law

Article 24: “Any person has the right to the protection of their private life.”

"Private communications, under whatever form that may be, are secret. Only justice can authorize, under the conditions and following the forms provided by the law, the access to their content, their total or partial divulgation or their summons [invocation] at the demand [charge] of whosoever."

Article 27: "The right to information may only be limited by the law, with the objective [but] of assuring the protection of all which concerns national defense, the internal and external security of the State, and the private life of persons, of preventing infringement to the fundamental freedoms and rights enounced in this Constitution and of protecting the sources and the domains determined with specificity by the law."

Article 28: "All have the right to express and to disseminate freely and within the sole limitsexpressly provided by the law, information, ideas and opinions."

The Moroccan Constitution of 2011 has been interpreted both as a defense of human rights as well as a specious attempt to bolster oppression while garnering international support as a stabilizing democracy. The rhetoric echoes liberal democratic sentiments and affirms what outsiders would define good governance, a category that many argue is a lifeline for the Moroccan state. All Moroccans are equal before the law. The judiciary is strengthened as an independent body. For the purposes of understanding what the document means for digital rights and the landscape of Internet freedom in Morocco, an analysis of Articles 24, 27, and 28, dealing with the rights to privacy and information must be made.

As is evident in the above excerpts from the constitution, individual rights to privacy and information are guaranteed to the extent that the law and the judicial system permit. Smith argues that these limits make the constitution mere rhetoric to impress international observers. In

practice, local organic laws are tied to the judiciary, an arm of the royal palace and state officials (Zaid, 2016). Although the constitution elaborates that the judiciary is independent, the king is still reserved the position of chair of the Higher Judicial Council (Smith, 2016). The judiciary also follows the Latin legal model from France, which contains a system of civil law rather than common law. The structure of a civil law system inherently privileges legal codes and legislative action over constitutional precedents (The Common Law and Civil Law Traditions).Thus, the Moroccan Constitution holds less power because legislation is the primary guide in judicial decisions.This fact relegates much authority to the judicial system, which is seen as weak and unqualified to understand technologyby some (MarouaneHarmach, personal communication, November 18, 2016). In any case,which legislation is guiding the judiciary on matters of digital rights and privacy?

Most laws affecting digital rights and Internet governance havedecreased personal privacy on account of national security. For example, the 2003 Law to Combat Terror expanded the power of Internet Service Providers (ISPs) and website owners to filter and delete content for the sake of national security and public order (Zaid, 2016). The law added to the Criminal Procedure Code and the Penal Code, providing a broad definition of terrorism and more serious sentences. Similar to the Patriot Act in the United States, this law justifies its provisions with the fear and uncertainty wrought by terrorism specifically after the bombings in Casablanca in May of 2003. Some human rights groups and the U.N.Committee against Torture have raised a red flag and accused the government of opening a secret detention center in Tamara where suspected militants are held and possibly tortured (Human Rights After the Casablanca Bombings, 2004). Digitally, the law has been invoked by the Attorney General to block news websites and arrest an editor accused of advocating terrorism (Zaid, 2016).

The Moroccan Press Code of 2002 also offers an example of repressive legal provisions that the state has used to monitor and prosecute journalists and activists online. In reality, the code expands the definition of incitement to crime and criminalizes any citizen found to have crossed a 'red line' as defined by Smith and Loudiy.Offenders are liable to 3-5 years imprisonment and fines from $800-$8,000 (Zaid, 2016). The legal framework having been defined, judges use the Press Code to prosecute citizens in the digital realm. Although it was removed from parliament, the *Digital Numerique* bill followed the legislative pattern by including justification for censorship of website deemed "inconsistent with the public political beliefs" (Kenyanito, 2015).

Applying the aforementioned laws in cyberspace falls to the ANRT.The ANRT was created as an independent body for liberalizing the telecommunications sector in 1998.Over time, it hasalso obtained law enforcement powers.Theking appoints the director and administrative board of the agency by *Dahir* or Royal Decree as is the tradition with most bureaucratic leadership positions. Because Maroc Telecom is the oldest telecom and controls the telephone cable infrastructure, the agency focuses on ensuring fair competition and access to the infrastructure by competitors Meditel and INWI (Zaid, 2016). The ANRT essentially promotes fairness for consumers as well as is evidenced in its reasoning to lift the ban. Scrutiny of the ANRT as an independent body has increased in light of the ban, the removal of its director general, and the lifting.

Surveillance and Civil Society

That the government conducts surveillance on Moroccan citizens is clear when looking at empiricalevidence.Western software companies have a track record of selling surveillance

technologies to countries in the MENA region, and Morocco is no exception (Noman& York, 2011). Leaked reports reveal that the Moroccan domestic intelligence agency, or DGST, has purchased surveillance software from Endace, a New Zealand company also found to sell surveillance tools to the U.S. and British governments (Gallagher& Hager, 2016). The purchase of these tools by the agency suggests that the Moroccan state is investing in domestic surveillance and jeopardizing citizen privacy. In 2011, the state was also revealed to have purchased a €2 millionsurveillance system named Eagle, produced by a French company and sold to the regime of Muammar Gaddafi (State of Privacy Morocco, 2016). Among other connections to foreign surveillance software, Access Now lists Morocco as one of the countries whose telecom companies have shown evidence of using mobile tracking headers to gather information on users (*The Rise of Mobile Tracking Headers: How Telcos Around the World Are Threatening Your Privacy*, 2015).If there had been doubts that the state has tried to spy on Skype conversations, a Citizen Lab report publishes evidence that Morocco has used FinFisher, a British-made technology that enables the secret recording of Skype conversations (State of Privacy Morocco, 2016).

Official documentation of these surveillance tactics increased in credibility with a provocative report issued by Privacy International. The reportdocuments the cases of four Moroccans who were put under digital surveillance by the government and experienced personal and professional harm because of their work. This report, which sparked a lawsuit by the Minister of the Interior, shows that the government as well as pro-government hacking groups have used cyberspace to spy on and intimidate journalists and activists.HishamAlmiraat, co-founder of the former citizen journalist website Mamfakinch and a digital rights activist, expresses his perspective in the report: “Repressive regimes have understood that the Internet is

not something to be left in the hands of citizens. They realized censorship is pretty obvious and so those companies are offering them a magic toy that instill fear among people and lead them to self-censorship. The very thought of being surveilled led people to decide by themselves to withdraw" (Their Eyes on Me: Stories of surveillance in Morocco, 2015).Mr. Almiraat's website, founded as a platform for the February 20th Movement, absorbed a Distributed Denial of Service (DDoS) attackin 2012, foreshadowing a rocky ending of the website (Their Eyes on Me: Stories of surveillance in Morocco, 2015). A few months later, many members of the editorial staff received a cryptic email that turned out to contain a piece of malware identified by its producer, Italian firm Hacking Team.Almiraat and the staffers reported the malware and discovered that it enabled the anonymous hackers with a keylogger and the ability to watch the cameras on certain computers(Their Eyes on Me: Stories of surveillance in Morocco, 2015).Other stories from the report discuss phone tapping and thesabotaging of social media accounts.

The production of this report in cooperation with a Moroccan non-governmental organization (NGO) evoked a pointed reprisal from the state.The NGO, theDigital Rights Association, wasfounded by Mr. Almiraat in 2014.After thereport gained attention, the Ministry of the Interior launched an investigation into the association and refused to allow registration of the organization with the state(Rida Ben Outhmane, personal communication, November 22, 2016).The state would not allow an association defending digital rights to gain recognitionas its actions proved to reveal too many undemocratic malfeasants. In order to continue pressing a digital rights agenda, the association transferred its work under the umbrella of the Moroccan Association for Human Rights (OMDH). Still, Mr. Almiraat has remained vigilant and active with Privacy International and Global Voices, an international community of bloggers and citizen journalists.Beyond the OMDH, the National Commission for the Protection of Digital

Rights (CNDP) actively monitors, studies, and analyzes digital rights in Morocco for the purpose of informing politicians and the public (Rida Ben Outhmane, personal communication, November 22, 2016).Even though these civil society groups manage to overcome the state's obstacles, they are limited.

In light of the treatment of the Digital Rights Association, many Moroccans have lost faith in the Internet as a safe space. This causes degradation in the number of voices in public debates, and theauthoritarian culture of fearsucceeds in eviscerating the democratic capabilities of the Internet. "The well was already poisoned and it was very hard to convince people that it was okay for them to participate online again,"Almiraat testified ("Securing Safe Spaces Online: Encryption, online anonymity, and human rights," 2015). In Lyon's terms, the panoptic model eroded public trust while increasing fear. Further validating the fear of citizens, Moroccan law on encryption technologies ambiguously requires registration with a military body in order to use encryption technologies ("Securing Safe Spaces Online: Encryption, online anonymity, and human rights," 2015). As Bruce Shneier argues, "Encryption is the most important privacy-preserving technology we have" ("Securing Safe Spaces Online: Encryption, online anonymity, and human rights," 2015). To what extent can Moroccans defend against state surveillance when the law limits the use of encryption?

Digital Public Opinion

Digital public opinion orthe collective discourse generated by citizens on social media platforms functions as an extra-state actor in contemporary Morocco. Facebook is the most widely used social media site with 12 million users while Twitter remains a platform used by mostly elites and professionals. YouTube occupies a position as the most powerful form of

television and overshadows the Moroccan mainstream media. With a solid foundation of these digital tools, digital public opinion revealed its potential force during the 2013 pardoning of a Spanish pedophile that had been sentenced to 30 years in prison. The pardon of Daniel GalvánViñasparked a wave of anti-state protests online tagged with‘#mafrasich’ (“I didn’t know” in Moroccan Arabic) and ‘#danielgate’ (Aay, 2013). The energy and persistence shown both online and in the streets led to the revoking of Viña’s pardon, but only after he had escaped to Spain (El Dahshan, 2013). What is significant about this event is that the digital public opinion was able to leverage the voices of people and provoke government action. The mainstream media, elite, and established political parties are effectively obligated to respond to citizens’ opinions, and the traditional “equilibrium” is disturbed (MarouaneHarmach, personal communication, November 18, 2016). These events reveal the existence of the democratic force of ICTs that the digital optimists have emphasized. Indeed, Moroccan digital activism today has some potential to push back against the state apparatus.

After the ANRT decision, it is no surprise that public awareness and discussion over social media was swift and forceful.Users protested by signing online petitions and organizing aFacebook “dislike” campaign to voice opposition against the three operators ---INWI, Maroc Telecom, and Meditel. Collectively, the operators lost approximately 600,000 likes on their Facebook pages even though they were quick to distance themselves from the regulation (Boujemi, 2016). This public activity and generation of opinion by digital means only heightens the pressure felt by the state following the Arab Spring and is likely a reinforcement of surveillance practices.

PERSPECTIVES

Throughout the time of this study, interviewees invoked three perspectives of the ANRT ban. The perspective of the ANRT, which can be categorized as a legal-economic perspective, holds that the ban served to protect the interests of the three telecom providers, Maroc Telecom, INWI, and Meditel. On anotherside, some believe that the UAE telecommunications giant, Etisalat, played a role in implementing the ban from its shareholding in Maroc Telecom. Finally, some suggest that the Moroccan security services influenced the decision. The lifting of the ban offers further insight into the decision-making of the ANRT and Moroccan politics.

ANRT Position

According to the ANRT, VoIP services like Skype"do not respond to the required legal gateway" (West, 2016). To the agency, the multinational companies providing the free services should have to obtain a license to operate in Morocco or pay some form of taxes. Indeed, in a communiqué justifying the ban, the agency cites a 2004 law that seeks to protect the telecommunications companies. The agency has also put forth the narrative that the ban is merely for the sake of promoting fair economic competition, a contention that the minister of industry, commerce, investment and digital economy corroborated(Freedom on the Net 2016: Morocco). Others argue that the government via Maroc Telecom and national corporations owns the telecommunications infrastructure and has a stake in revenue (Mohapi, 2016). Indeed, the state owns 30 percent of Maroc Telecom in addition to the national railroad and national electricity and water utilities, controllers of 16,000 km of fiber-optic cables (Freedom on the Net 2016: Morocco).

Some literature validates this position.Timothy Wu looks at China and Mexico wherethe governments had blocked VoIP services and been active in regulating cyberspace. He concludes with acceptance of the economic reasoning: "Leaving censorship aside, it is also true that some Internet filtering, like the blocking of Internet-based telephony discussed within, seems to have little to do with political control and much more to do with the protection of domestic incumbents" (2006). This research aside, interviews yielded a critical perspective of the official ANRT reasoning.

One interviewee explained that the ban came out first on 4G services, which had been introduced to the market just three months earlier. The ban was subsequently implemented city by city and without an official announcement by the ANRT. From this information, the interviewee believes that the problem of the telecom operators becomes "clear." VoIP usage over 4G likely increased and caused a quality of service issue for telecom networks. The thinking goes that the quality of service as a whole decreases for all cell phone users because VoIP calls over 4G puts a strain on the network. Be it a technically sound framing, he calls it an "alibi." He also discounted the ANRT's reasoning from the fact that most Moroccans already do not subscribe to monthly telephone plans. Even so, the number of Moroccans that initiate international calls is very low because family or friends abroad most often attain more financial resources or access to free online calling. Anecdotally, it seems that the ban must not have been

For another professional, the ANRT's explanation for the ban simply does not provide the full picture. An IT consultant and digital media expert shared his disbelief in the logic: "I objectively don't understand the decision…data is the future of telecom, not voice" (MarouaneHarmach, personal communication, November 18, 2016). He also mentioned speaking to a representative at a telecom company who said that the company did not support the

ban because VoIP services actually benefit them. This anecdote, along with the retaliatory statements of Meditel and INWI, provides fodder for debate and looking beyond the official reasoning.

Etisalat and Multinational Business

From a less popular perspective, the ban may be linked to the UAE-based telecom company that owns a 53 percent stake in Maroc Telecom. Etisalat purchased its stake in Maroc Telecom in 2014 and now operates in 15 countries throughout the Middle East, Africa, and Asia (Bianchi & Khan, 2014). The corporation has a history of disrespecting principles of net neutrality and access to information, having also allowed the blocking of Facebook's Free Basics service in Egypt this year (Micek, Olukotun, &Chennoufi, 2016). Connecting the ANRT's decision to Etisalat also gains credibility from a report released by Ali Amar at *Le Desk.* Amar questions the sacking of the former ANRT director general and recalls that the removal of high-level government officials typically results after a public decision by the king (2016). He suggests that something more must have contributed to the sudden removal, possibly a shareholder agreement extending decision-making authorities to Etisalat. If the Emirati shareholders via Maroc Telecom were involved in the director's dismissal, it is possible that they also swayed the ANRT's decisions. The UAE has experienced its own saga of VoIP banning and conflicts between its regulatory agency and two telecom operators, one of which is Etisalat (Samoglou, 2016).

The Moroccan state and the UAE share a business culture as well as bilateral relations on military and intelligence matters. Extending the comparison to other business-orientedcountries in the MENA region, Oman, Kuwait, Saudi Arabia and Egypt have also blocked VoIP services

(Ben Mehrez, 2016). No direct correlations can be established; however, bilateral and multilateral cooperation and business culture offer reason to draw the connection of these top-down decisions. The evidence connecting Etisalat and the removal of the former ANRT director shows that the multinational company has room to exercise power. Whether the other MENA countries blocked services for economic, security, or country-specific purposes, there is a trend helping to fill in the gaps of the ANRT's actions.

Security and the DGST

Connecting the Moroccan security services to the ANRT's decision is the least documented of the post-ban discussion topics. It is true that similar circumstances have been studied in Egypt where Skype's encryption capability was seen as burden to the security services (Bryant, 2012). However, the lack of overt discussion in Morocco demands speculation based on the context of digital public opinion, surveillance, and the February 20th Movement. To be clear, there remains no direct correlation between the ANRT ban and the security services. No official statement after the introduction and removal of the ban mentioned security. Still, influencers and professionals in information technology note that there is state "awareness" recognizing the security implications of social media and its use as a networking tool for crime and terrorism. That "the services are more suspicious of the Internet" most certainly stems from the role that social media played in empowering and advancing the Arab Spring (MarouaneHarmach, personal communication, November 18, 2016). One interviewee speculated that the Moroccan intelligence agency or DGST undergirds the decision even though the ANRT neglected to admit them (Ali Elouafiq, personal communication, November 24, 2016). When considered alongside

the sacking of the former ANRT head and the aforementioned context, this claim begets attention.

If the DGST coopted the VoIP ban, what would have motivated it to do so? First, Morocco has a national security issue with Islamic State cells particularly in the northern Rif region. Reports have shown that the agency has actively thwarted many attacks and even cooperated with foreign governments such as France (Morocco provided intelligence to help France in Paris raids: Sources, 2015). Logistically, the DGST would have an interest in minimizing communications in order to prevent terrorists from networking and coordinating attacks. This begs the follow-up question: why would the agency want to ban VoIP services specifically? Technically speaking, filtering VoIP communications is very expensive and time-consuming (Ali Elouafiq, personal communication, November 24, 2016). In order for a call to begin, the Session Initiation Protocol (SIP) must be followed, but thereafter, eavesdropping on the call is impossible. It would be technically practical for the DGST to lobby for or demand the complete banning of VoIP services. Users are then forced to use services that the agency can more easily filter including Virtual Private Networks (VPNs). In fact, many circumvented the VoIP ban by using VPNs, yet these applications make it easier for authorities to track communication endpoints.

CONCLUSION

Connecting the perspectives above to the context of cybersecurity in Morocco, the ANRT ban of VoIP fits into a larger discussion of surveillance and privacy in cyberspace. The aid of Lyon's panoptic model helps to conceptualize surveillance and the effect it has had in spreading self-censorship in Moroccan society. Discussions with colleagues and interviewees confirm that

self-censorship permeates daily life and is a testament to Moroccan culture and the state's incitement. Accounting for the presence of censorship in Moroccoand its semi-authoritarian habits, Shirky's "conservative dilemma" helps explain the realities in Privacy International's report and the formidability of digital public opinion. It is in this context that the ANRT's perspective must be weighed against the explanations involving Etisalat and the security services.While fleshing out a single explanation may be impossible, this study draws attention to the many factors of the decision. If expert opinion holds any weight, business interests and state security concerns contributed to the decision. The lifting of the ban is a step in the right direction, but Moroccans must remain vigilant to future efforts against privacy.

ACKNOWLEDGEMENTS

I would like to express my gratitude to MarouanneHarmach, RidaBen Outhmane, and Ali Elouafiq for their time and invaluable insights for this project. I would also like to express thanks to my research DrissKsikes for his guidance in framing this project and pursuing research. Last but not least, I thank TaiebBelghazi, NawalChaib, and the staff at the Center for Cross Cultural Learning for providing the recourses and guidance that enabled this project.

شكرا!

REFERENCES

Aay, A. (2013, August 10). Morocco: “Daniel Gate” Sparks Unprecedented National Outrage. Retrieved November 23, 2016, from https://globalvoices.org/2013/08/10/morocco-daniel-gate-sparks-unprecedented-national-outrage/

Accuséd'espionnage au Maroc, le ministère de l'Intérieurporteplainte. (2015, May 8). Retrieved November 26, 2016, from http://www.h24info.ma/maroc/politique/comment-le-maroc-empeche-le-printemps-arabe-en-espionnant-ses-citoyens/32846

Amar, A. (2016, October 28). Affaire ANRT : La règle de droitsacrifiéesurl'auteld'inavouables intérêtsstratégiques? Retrieved November 26, 2016, from https://ledesk.ma/enclair/affaire-anrt-la-regle-de-droit-sacrifiee-sur-lautel-dinavouables-interets-strategiques/

Ben Mehrez, H. (2016). Mapping VoIP Service Provider Blockage in the MENA Region. Retrieved November 2, 2016, from https://www.igmena.org/index.php?p=533

Bianchi, S., & Khan, S. (2014, May 5). Etisalat Moves West Africa Units to Maroc Telecom It's Acquiring. Retrieved November 26, 2016, from https://www.bloomberg.com/news/articles/2014-05-05/etisalat-agrees-to-sell-west-africa-businesses-for-650-million

Boujemi, Hanane. "VOIP Ban in Morocco: The Battle of Telecoms Survival." *LinkedIn*. N.p., 8 Apr. 2016. Web. 23 Oct. 2016.

Bryant, E. I. (2012). The iron fist vs. the microchip.Journal of Strategic Security, 5(2), 1-26.

El Dahshan, M. (2013, August 9). Moroccans Finally Said It: “The King Is Pardoning

Pedophiles". Retrieved December 01, 2016, from http://foreignpolicy.com/2013/08/09/moroccans-finally-said-it-the-king-is-pardoning-pedophiles/

Freedom on the Net 2016: Morocco. (n.d.). Retrieved November 26, 2016, from https://freedomhouse.org/report/freedom-net/2016/morocco

Gallagher, R., & Hager, N. (2016, October 23). The Little-Known Company That Enables Worldwide Mass Surveillance. Retrieved November 19, 2016, from https://theintercept.com/2016/10/23/endace-mass-surveillance-gchq-governments/

Human Rights After the Casablanca Bombings.(2004, October). Retrieved November 24, 2016, from https://www.hrw.org/reports/2004/morocco1004/4.htm

INWI Withdraws from Maroc Web Awards After ANRT Banned Skype, FaceTime. (2016, March 2). Retrieved October 24, 2016, from https://www.moroccoworldnews.com/2016/03/181145/inwi-withdraws-from-maroc-web-awards-after-anrt-banned-skype-facetime/

Kenyanito, E. (2015, February 13). Emerging threats in cybersecurity and data protection legislation in African Union countries. Retrieved November 29, 2016, from https://www.accessnow.org/emerging-threats-in-cybersecurity-data-legislation-in-africa-union/

Lyon, D. (1994). *The electronic eye: The rise of surveillance society*. Minneapolis: University of Minnesota Press.

Micek, P., Olukotun, D., &Chennoufi, A. (2016, January 06). Etisalat shuts off internet services in Egypt andMorocco. Retrieved November 26, 2016, from https://www.accessnow.org/etisalat-shuts-off-services-in-egypt-and-morocco/

Mohapi, T. (2016, January 25). Why Did Morocco Ban VoIP & Why Is South Africa Looking To Regulate OTT Services? Retrieved November 18, 2016, from http://www.iafrikan.com/2016/01/25/why-did-morocco-ban-voip-why-is-south africa-looking-to-regulate-ott-services/

Morocco provided intelligence to help France in Paris raids: Sources. (2015, November 18). Retrieved November 16, 2016, from http://www.reuters.com/article/us-france-shooting-morocco-idUSKCN0T729X20151118

Morocco's Constitution of 2011. (n.d.). Retrieved November 24, 2016, from https://www.constituteproject.org/constitution/Morocco_2011.pdf?lang=en

Morocco's VoIP Ban Quietly Reversed Without Official Announcement. (2016, October 24). Retrieved October 30, 2016, from https://www.moroccoworldnews.com/2016/10/199712/moroccos-voip-ban-quietly-reversed-without-official-announcement/

Noman, H., & York, J. (2011, March). West Censoring East: The Use of Western Technologies by Middle East Censors, 2010-2011. Retrieved December 01, 2016, from https://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011

Samoglou, E. (2016, April 18). UAE telecoms companies told to free up internet calling. Retrieved November 24, 2016, from http://www.thenational.ae/uae/uae-telecoms-companies-told-to-free-up-internet-calling

Securing Safe Spaces Online: Encryption, online anonymity, and human rights (Rep.). (2015, June). Retrieved December 1, 2016, from Privacy International website: https://www.privacyinternational.org/sites/default/files/Securing Safe Spaces

Online_0.pdf

Shirkey, C. 2011. The political power of social media: technology, the public sphere and social change. Retrieved November 28, 2016 from http://www.foreignaffairs.com/articles/67038/clay-shirky/the-political-power-of-social-media.

Smith, A. (2016). Transformational Pragmatics in the Mena Uprisings: Re-Territorialization in Morocco. In *Communication and conflict transformation through local, regional, and global engagement*. Lanham, MD: Lexington Books.

Smith, A. R., &Loudiy, F. (2005, August). Testing the Red Lines: On the Liberalization of Speech in Morocco. Human Rights Quarterly, 27(3), 1069-1119.

State of Privacy Morocco. (2016, November 4). Retrieved December 01, 2016, from https://privacyinternational.org/node/971

The Common Law and Civil Law Traditions. (n.d.). Retrieved November 28, 2016, from https://www.law.berkeley.edu/library/robbins/CommonLawCivilLawTraditions.html

The Rise of Mobile Tracking Headers: How Telcos Around the World Are Threatening Your Privacy (Rep.).(2015, August). Retrieved November 26, 2016, from Access Now website: https://www.accessnow.org/cms/assets/uploads/archive/AIBT-Report.pdf

Their Eyes on Me: Stories of surveillance in Morocco. (2015, April 7). *Privacy International*. Retrieved October 30, 2016.

West, D. M. (2016, October). Internet shutdowns cost countries $2.4 billion last year. Center for Technology Innovation at Brookings. Retrieved October 23, 2016, From https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf.

Wu, T. (2006). The world trade law of censorship and internet filtering. Chicago Journal of International Law, 7(1), 263-287. Retrieved from http://proxygw.wrlc.org/login?url=http://search.proquest.com/docview/237216263?accountid=11243

You Can Make Skype Calls in Morocco Again. (2016, November 04). Retrieved December 01, 2016, from http://fortune.com/2016/11/04/morocco-skype-ban/

Zaid, B. (2016, January 25). Internet and democracy in Morocco: A force for change and an instrument for repression. *Global Media and Communication,12*(1).

APPENDIX: Informed Consent for Individual Interviews

Purpose: You are being asked to participate in a research study conducted byTyler Delhees from George Washington University. The purpose of this study is tomap Moroccan perceptions of the ANRT's decision to ban VoIP services particularly Skype. This study will contribute to the completion of my Independent Study Project.

Research Procedures

Should you decide to participate in this research study, you will be asked to sign this consent form once all your questions have been answered to your satisfaction. This study consists of an interviewthat will be administered to individual participants in an agreed-upon public location. You will be asked to provide answers to a series of questions related to Internet rights and the ANRT ban of VoIP services. With your permission, you will be audio taped.

Time Required

Participation in this study will require 30 minutes of your time.

Risks

I do not perceive any risks or more than minimal risks from your involvement in this study; however, should you feel uncomfortable or unwilling to complete the interview process, you are able to withdraw at any time.

Benefits

Potential benefits from participation in this study include gaining knowledge on the status quo of Internet rights and governance of the Internet in Morocco. Each participant will be offered an electronic copy of the final project or a summary of results.

Confidentiality

The results of this research will be documented as an ISP paper and presented orally to the SIT MOR students and staff. The results of this project will be coded in such a way that the respondent's identity will not be attached to the final form of this study. The researcher retains the right to use and publish non-identifiable data. While individual responses are confidential, aggregate data will be presented representing averages or generalizations about the responses as a whole. All data will be stored in a secure location accessible only to the researcher. Upon completion of the study, all information that matches up individual respondents with their answers (including audio tapes, if applicable) will be destroyed.

Participation & Withdrawal

Your participation is entirely voluntary. You are free to choose not to participate. Should you choose to participate, you can withdraw at any time without consequences of any kind. You may also refuse to answer any individual question without consequences.

Questions about the Study

If you have questions or concerns during the time of your participation in this study, or after its completion or you would like to receive a copy of the final aggregate results of this study, please contact me at tdelhees@gwmail.gwu.edu or +212 6 96 67 81 66.

Researcher's Name: Tyler Delhees

Giving of Consent

I have read this consent form, and I understand what is being requested of me as a participant in this study. I freely consent to participate and have been given satisfactory answers to my questions. The investigator provided me with a copy of this form, and I certify that I am at least 18 years of age.

☐ I give consent to be audio taped during my interview. _____ (initials)

_____

Name of Participant

_____ _____

Name of Participant (Signed) Date

_____ _____

Name of Researcher (Signed) Date

Déclaration de consentement

L'objectif d'étude

Le but de cette étude est d'interpréter les perceptions morocaine de le decision de l'ANRT d'interdit les services de voix sur IP Skype en particulier. Cette étude contribuera à mon projet d'études indépendantes.

La durée et les éléments d'étude

Cette étude sera dirigée pendant une période de trois semaines. L'étude inclura les observations et les interventions des participants en incluant leur travail sur terrain.

Les risques

L'étude n'a aucun risque prévisible pour les participants. Cependant, si vous ne vous sentez pas confortable avec le procédé d'observation ou d'interview, vous êtes libre de terminer votre participation.

Compensation

La participation à cette étude ne sera pas compensée, financièrement ou autrement. Cependant, votre aide est considérablement appréciée par notre équipe de recherche.

Confidentialité
Tout effort de maintenir votre information personnelle confidentielle sera fait dans ce projet. Vos noms et toute autre information d'identification seront changés dans la description finale, et seulement connue à l équipe de recherche.

Participation
Je soussigné, …….., confirme avoir lu les rapports ci-dessus et compris que ma participation à cette étude est volontaire tout en ayant la liberté de retirer mon consentement à tout moment sans pénalité.

_____ _____
Signature Date

J'ai pris conscience que cette étude puisse comporter les entrevues et/ou les observations qui peuvent être enregistrées et transcrites.

_____ _____
Signature Date

Team de recherche

Les chercheurs peuvent être contactés par E-mail ou téléphone pour n'importe quelle raison ;