Mapping Controls on Digital Information in Jordan

CYBER STEWARDS

Mapping Controls on Digital Information in Jordan

7iber Dot Com

in partnership with

Citizen Lab

Munk School of Global Affairs

University of Toronto

Researcher:

Reem Almasri

Co-researchers:

Issa Mahasneh

Mohammad Tarakiyee

TABLE OF CONTENTS

I.

Executive Summary

Many aspirations were built on the Internet as a driver for the Jordanian economy when the Internet first arrived in Jordan. In 2000, a national reform across education and the labor market was launched by the royal family to transform the country into the hub of information and communications technology (ICT) in the Middle East. While creating emerging markets dependent on the Internet was the main purpose of this national plan, it also led to the decentralized production of mass media content away from state-controlled media. While the state was committed to promoting an open Internet market, its relationship with regulating the online content went through phases, depending on the unaccounted threats that they posed to the state.

Investing in technology entrepreneurship and content enterprises, and creating an ICT stream in schools and universities was seen as the only way to embark on the economic opportunity that the Internet could bring to the country. As a byproduct of this ICT-infused economy, many Arabic Web social platforms sprung up from Jordan, such as IKBIS, Jeeran, and Maktoob. The latter was sold to Yahoo for 19 million dollars in 2009.[1] By 2012, Jordan ranked forty-seventh in the Networked Readiness Index, and sixth regionally; it became home to 450 ICT companies, and the ICT industry contributed 14% of the country's GDP.[2] According to the International Telecommunications Union (ITU), 75% of the online Arabic language content originated in Jordan.[3]

Aside from a new ICT market, the increased Internet penetration also facilitated a boom of electronic news websites and blogs that often told a different story from that of official mainstream media. These developments paved the way for 400 news websites to emerge by 2013. As the waves of revolutions around the region unfolded, citizens flocked to alternative news sources—Facebook was one of the most visited sites. The era also saw a dramatic increase in Facebook users, which in 2013 reached 2.6 million users in Jordan, of whom 67% were between eighteen and thirty-five years old.[4] In Jordan, the increased penetration rate, the rise in regional oppositional voices, and the rise in Facebook users facilitated the creation of alternative spaces that raised the bar of free expression and publicly questioned the government and the monarchy's plans for political, economic, and social reform. Many of the issues that were deemed taboo among citizens and mainstream print media were now being tackled and discussed online.

Official attempts to control online speech and expression contradicted the progressive image of an open ICT market in Jordan to encourage global investment. For example, just a year after passing amendments on a press and publication law in Dec 2012 which resulted in blocking 300 websites, king Abdullah II was on a trip to the United States with Jordanian entrepreneurs to promote Jordan as the Silicon Valley of the Middle East.[5] The constant effort in ignoring the impact of content controls on the ICT market is often countered by numbers on the shrinking of such market. A survey conducted by the Information and Communication Association of Jordan reported the closure of 100 companies between the years of 2012 and 2013. Press and publication law was considered one of the legislative restrictions attributed to discouraging ICT businesses in Jordan[6].

1YahooAcquiring Arab Portal Maktoob," *The Guardian*, 25 August 2009. Accessed 26 August 2013, http://www.theguardian.com/media/pda/2009/aug/25/yahoo-internet.

2 "Global IT Report: Living in a Hyperconnected World," *World Economic Forum*, 2012.

3 Samir Aita and Abdulilah Dewachi, "Status of the Digital Arabic Industry in the Arab Region," UN Economic and Social Condition for Western Asia (ESCWA), 2012. Accessed 20 March 2015, http://www.escwa.un.org/information/publications/edit/upload/E_ESCWA_ICTD_12_TP-4_E.pdf

4 Rana Swies and Dina Baslan, "Mapping Digital Media: Jordan," Open Society Foundations, 2013. http://www.opensocietyfoundations.org/reports/mapping-digital-media-jordan.

5 "Jordan's King Abdullah II to Talk Technology and Startups at UC Berkeley," *San Francisco Business Times*, 13 May 2014, http://article.wn.com/view/2014/05/13/Jordans_King_Abdullah_II_to_talk_technology_and_startups_at_/

6 Mbayddin, I, "One Hundred Companies out of the ICT Market" Alghad Newspaper, 1 October 2013, available at

In a country that barely survived the political upheaval of the Arab revolutions, and which is currently exhausting all measures to protect its security in the middle of neighbouring turmoil, the conversation about how access to information is governed in Jordan has not yet reached the public domain. This paper attempts to map government-mandated control mechanisms on access to and production of digital content over the past five years ever from the time of the writing this paper. It explores how these controls are strengthening constraints on basic human freedoms, such as expression and privacy—the main freedoms in building any open, democratic, and progressive society.

This paper examines which entities have the power to control access to the Internet, and the production of content online, especially during a period of heightened political awareness and the widespread use of social-networking tools. Our documented cases of censorship and persecution of online speech provide evidence for human-rights entities interested in the politics of regulating online content in Jordan. This research also highlights huge gaps in policy-makers' understanding of the Internet's infrastructure and technical design, which is an important issue to take into consideration for future legislation.

Main Findings

In Jordan, several public and private entities have overlapping executive and legislative jurisdictions over the production and access of content. As granted by the Press and Publication Law, the director of the Press and Publication department has the jurisdiction to administratively explain the law and list websites that require licensing. Another example is the ISPs' authority to administratively suspend a service if it is proven to violate public morals or the public conduct. Certain ISPs have practiced de facto blocking on some websites without any official or judiciary request. The lack of a judicial process in regulating content removes citizens' right to legally challenge the blocking order, given that it was based on the personal diligence of the press and publication director and the ISPs.

- While some information controls are practised through the rule of law, the most effective are practised informally. The weak system of accountability, the lack of judiciary review, in addition to the unregulated intimidation mechanisms from the intelligence department, intensify self-censorship. The lack of transparency in explaining and applying the laws, and the lack of checks and balances make for uncontested intervention by the Ministry of the Interior, General Intelligence Department, National Information and Technology Center (NITC), and ISPs in access and production of digital information. Surveys report that 85% of journalists avoid writing about topics critical of the regime, religions, and Gulf governors. Responses from surveys and focus groups link surveillance to digital self-censorship. These informal mechanisms of control have proven to be the most effective constraint on information.

- The application of formal blocking requests reflects the extent to which ISPs are participating in applying further controls beyond the minimum requirements of the blocking orders. ISPs' choice of blocking technique could reflect both their own blocking mentality, and the available technologies and equipment in the ISPs network that could stand between the user and the website that s/he attempts to access. We also detected the use of a more complicated technique on one ISP which injected fraudulent TCP reset packets to block access to websites. This technique is less transparent to the average user and reflects a greater technical sophistication than DNS tampering.

- Legislations regulating online content lack technical understanding of the Internet's working and make for a confused application of law. For example, the attempt to draw local borders on digital content in an interconnected network have intensified the labor needed to categorize emerging websites to electronic websites that require licensing and implement a

<**https://tinyurl.com/lzjnut2**

blocking order. Information Crimes Systems law is another place this gap in legal terminologies and technical realities of the Internet is present. The law criminalizes any illegal or unauthorized entry to a website—any website. This disregards the essential feature of websites being public in their nature without requiring an authorization for access. All efforts to apply the law on what is defined as local still do not guarantee a solid implementation.

II. Introduction

The evolution of the Internet in Jordan tells the story of a delicate balancing act between official efforts to position the country as the regional hub for ICT, and the state's internal endeavours to enforce control on the natural flow of information that the Internet provides.

Like elsewhere in the world, the Internet boom in Jordan and hike in penetration rates has led to the emergence of new decentralized narratives that question the state's mainstream narrative. These new narratives in news websites, blogs, and political pages on Facebook provide different stories than state-owned TV channels and radio stations tell. With every publishing platform, the Jordanian government places solid controls on the flow of information, but the rules of the game are different for a platform as lucid and interconnected as the Internet. Books, movies, newspapers, TV stations, and radio channels have always been successfully monitored and managed by the Jordanian state applying rigid censorship rules. These monitoring processes were not labor intensive and were practical. For example, a committee in the Press and Publication department specializes in reviewing books and movies flowing into the country and approving what complies with certain rules. Books that insult the regime, offend "divine" religions, or disrupt friendly relationships with other countries are banned. The same goes for movies in cinemas. Films are continuously subjected to censorship by removing scenes that disrupt public morals.[7] Newspaper publishers have assigned intelligence department officers to filter content before the paper goes to print[8]. TV stations and radio channels have to obtain a high-cost license from the Audio and Visual Department if they tackle political programming. State control practices involving information take the shape of formal legislation and informal but officially agreed upon rules.

While the Jordanian state implemented major changes in the educational sector and privatized the telecom market to position Jordan as the hub of ICT in the region, it did not predict the unintended consequence of rising threats to its mainstream narrative. Privatization of telecommunication and Internet Service Providers, the growing labour specialized in web development, and high Internet usage, led to the decentralization of publishing platforms. The new borderless network with its lucid publishing platforms has made legacy information controls inefficient. This has changed the rules of information control for the state, which is now investing in stronger formal and informal techniques.

This research attempts to map government-mandated and government-influenced control mechanisms on access to and production of digital content. It explores how these controls are strengthening constraints on basic human freedoms, such as expression and privacy—the main freedoms in any open, democratic, and progressive society. It attempts to demystify the official narrative that detaches the building of a vibrant Internet market from an environment that encourages free expression.

This research documents different entities and their jurisdiction on production of and access to online information. It examines closely who has the power to control access to the Internet, and the production of content online, especially during a period of heightened political awareness and the widespread use of social-networking tools. The documented cases of censorship and persecution of online speech provides valuable information for human-rights entities interested in the politics of regulating online content in Jordan. This research highlights huge gaps in policy-makers' understanding of the Internet's infrastructure and technical design, which is an important issue for future legislation. This lack of understanding is evident in the inadequacy of definitions and legal terminologies used in the legal framework that describes the application of laws regulating the Internet.

7 "Banning Books in Jordan: Custody of the Reader and Dismissing Law" [in Arabic], 6 February 2014, 7iber, available at http://www.7iber.com/2014/02/jo-book-censorship/

8 "Security Apparatus: leaving its square...limiting freedoms" [in Arabic], 25 July 2012, Amman Net, available at ar.ammannet.net/documentary/news/456/

Finally, by mapping digital control in Jordan, this research also hopes to open up future research and discussion on how the Internet should be regulated across multiple players, given its never-ending technical development.

To achieve these objectives, the research classifies these controls as formal and informal ones practised over the past ten years of the Internet's life in Jordan. It first maps out formal techniques—the visible techniques that lie in the legislative framework that both vaguely calculates free zones for online expression, and grants accessibility to certain publishing platforms online inside Jordan. The legislative framework draws these legal free-expression zones first in expanding limitations on speech to online platforms through laws in the Penal Code, the Press and Publication Law, the State Security Court law, the Information Systems Crimes law, and Anti-Terrorism law. In addition to delineating legal free-expression zones, legislative frameworks also control the very access to online publishing platforms through the 2012 amendments to the Press and Publication Law. We also explore the informal techniques for exercising control over access to and production of digital content that exist outside the official legislative framework. Informal control is executed by different state and private entities through internal regulations that are not subject to public scrutiny, discussion, or judicial review. These entities are the General Intelligence Department, the Ministry of the Interior, the ICT departments of public universities and ministries, as well as ISPs themselves. We then examine further technical controls found in ISPs' application of blocking orders which place a third layer of informal control on the right to access information, all under the name of protection from legal liability. We draw connections between formal and informal controls and people's actual experiences based on online surveys, focus groups, and interviews with lawyers and journalists. Separating the results from an online survey highlight the implications of these formal and informal tools on the online users' experiences.

Finally, we explain the results of technical testing that uncovers another layer of informal controls practiced by telecommunication companies.

III. Methodology

To map the current formal and informal factors that affect access to and production of content in Jordan we conducted a series of interviews, online surveys, focus groups, and policy and literature analysis.

***Policy Analysis*:** To trace online restrictions on speech we collected public court cases on online speech and analyzed the following laws and regulations in their current format after amendments:

- The Press and Publication Law (1999);
- The Penal Code (1960);
- Information Systems and Cyber Crimes Law (2013);
- The Telecommunication Law (1995);
- State Security Law (1959)
- Anti-Terrorism Law (2006)
- Internet Cafes regulations (2008 Ministry of the Interior).

Semi Structured Interviews: Interviews were conducted with lawyers, journalists, and Internet cafe owners to explore the translation of laws, legislation, and regulations on Internet content and online user experience.

- Lawyer Leen Khayyat on court cases on online expression;
- Lawyer Mohammad Qutaishat on the state of the Press and Publication Law;
- Lawyer Adel Saqf al-Hiet on the Google case and the ISPs case;
- Journalists Mohammed Omar, Sawsan Zaydeh, and Lina Ejeilat;
- Four bloggers (who would rather remain anonymous);
- Four Internet cafe owners from the town of Irbid in northern Jordan.

Network Measurement: The research team partnered with the Citizen Lab from the University of Toronto to conduct network measurement experiments designed to gather evidence of Internet filtering on four Internet service providers in Jordan in June 2013 and August 2014. These tests' findings highlighted the number of blocked websites that ISPs filtered in response to a blocking order in June 2013, and during the period of June 2013 to August 2014. Most importantly, these findings revealed the filtering techniques that each ISP used to perform the blocking orders.

***Online Surveys*:** Two online surveys were developed and posted on 7iber's website. One survey targeted general online users and the other targeted university students specifically. Although these two surveys were not representative of the online user population, they aimed to highlight emerging trends in the informal restrictions on online speech. The first survey aimed to explore perceptions of surveillance online and how it changes users' online behavior when accessing or creating content. The survey for university students explored different surveillance practices that universities apply on their networks, and how these practices influence students' usage of the local university network.

Focus Groups: Three focus groups were conducted with university students in Irbid, Karak, and

Amman. The purpose of these focus groups was to delve deeper into students' perceptions and experiences with surveillance on different networks and its impact on freedom of speech. Participants were required to be frequent Internet users between the ages of eighteen and twenty-two.

IV. Overview

Internet Infrastructure:

As of March 2014 there are thirteen Internet Service Providers in Jordan providing connection to businesses and homes through ADSL, 3G, Wimax, leased lines, VPNs, and Frame relay. The Orange Jo, Zain, and Umniah telecommunication companies have the highest share of Internet subscriptions, given that 3G subscriptions constitute 70% of overall Internet subscriptions. However, over the past few years, the Internet market has witnessed the rise and fall of ISPs as a by-product of either emerging new connection technologies, or the semi-monopoly of Orange Jo on the fixed broadband network.

The fixed broadband market is not as vibrant as it was expected to be, given the market's liberalization. The privatization of what was called Jordan Telecom into Orange Jo in 2000 made Orange Jo the exclusive owner of the bundled public switched telephone network (PSTN) infrastructure, the national IP backbone, and the international connections. Any companies that needed to provide fixed broadband connection had to interconnect with Orange's core IP network and rent Orange's bundled PSTN at high fees. This created an uncompetitive environment that discouraged new entry, which led many ADSL ISPs to shut down and the cost of access to remain high.

There are seven companies providing ADSL (of which three are telecom) compared to thirteen ISPs companies in 2011.[9]

Turbulence hit Jordan's Wimax market that was introduced in 2008. Before the introduction of 3G, Wimax was a good alternative for ADSL's high cost and lack of coverage especially in certain under-serviced areas. The higher coverage of 3G and the larger mobility put the Wimax market at risk. ISPs like WhiteTribe and Kulacom who provided only Wimax as a product shut down. [10]

It is hard difficult to pin down an Internet penetration rate in Jordan, given the discrepancy in reporting by the two government institutions surveying Internet usage: the Telecommunication Regulatory Commission (TRC) and the Department of Statistics (DOS). In a survey done on technology usage in households, the DOS reported that the penetration rate in 2012 was 43%. On the other hand the TRC reports a penetration rate of 67% for the same year. The TRC's percentage for 2014 was 73%.[11]

While it is hard to confirm penetration rate according to the different formulas that different official entities use in Jordan, tThe subscription rate of each connection type may present a better picture of the extent that the Internet is accessible in Jordan. The ITU reported that in 2012 fixed broadband penetration was at 3% compared to 11.8% for active mobile broadband penetration. This wider spread of mobile penetration is reflected in the TRC's distribution of subscription shares according to connection type. The TRC reported that mobile broadband held 70% of subscription shares. The shares of ADSL (17%) came second and Wimax (10%) came third in the total Internet subscription number.

---

9 "ICT Adoption and Prospects in the Arab Region (Report)," ITU, 2012 available a:http://www.itu.int/pub/D-IND-AR-2012

10 "WhiteTribe Ends Its Services in Jordan" [in Arabic], *Sinarah News*, 3 October 2013, http://www.snarah.net/index.php/news/ar/2228-jordan1024; "Kulacom Jordan Leaves the Market" [in Arabic], Zad News, 4 March 2014, http://www.jordanzad.com/index.php?page=article&id=151525

11 Department of Statistics, http://www.dos.gov.jo; Telecommunication Regulatory Commission, http://www.trc.gov.jo/ [in Arabic].

The introduction of mobile broadband connection (3G) in 2010 affected subscription rates for other connection types. ADSL dropped from 32 to 17% of Internet subscription shares between the years of 2011 and 2013. The share of Wimax connections significantly dropped as well during these years.

Online News Development

It was not until 1996 that Internet access was available in Jordan with dial-up connections being the only method to connect. The low penetration rate and high cost of access restricted the adoption of the Internet as a platform to consume or produce information in Jordan: journalists and citizens were still getting introduced to the new technology. The lack of Arabic-language-supported platforms delayed online news websites from getting established in Jordan or elsewhere in the region. In 1998, Maktoob Dot Com attempted to develop an Arabic online hub for blogs, e-mail, and other digital tools. The portal came at the right time because more people were starting to use personal computers. Maktoob introduced an Arabized portal embracing concepts of online communities, blogging, and online journalism in Jordan and around the region. In 2000, the Al Bawaba regional portal followed, focusing on the production of online news by prominent Jordanian journalists.

The continuous drop in Internet connection costs, the increase in its penetration rate, and the development of Arabic-language-supported tools encouraged Arabic newspapers to establish their presence in the online sphere. The Jordanian newspaper *Ad-Dustour* was the first to have its daily newspaper posted online. In 2003, the first Arabic online radio, Ammannet, started broadcasting from Amman because they couldn't obtain a traditional radio license at the time. Between 2003 and 2005 many Arabic news websites arose and fell—the cost of running the sites was still relatively high. However, the government's support of Internet access in universities and public institutions in 2005 increased the Internet penetration rate, giving incentives to news websites and content production companies to launch.

The fact that readers were able to share content, and challenge and discuss mainstream news increased online forums and the blogging scene. In 2005, online social forums and blogs in the region supported websites such as *Al Jazeera Talk*, which gained in popularity. The blogging community in Jordan grew, reaching 500 blogs in 2007 and covering a wide spectrum of political and social topics in both Arabic and English. The same year also marked the rise of local online news websites. *Ammon News* was the first e-news website to publish original local news, breaking the monopoly of mainstream media. The continuous drop in the cost of running a news website and the crackdown on printed tabloids in Jordan increased the reach of Internet-based news sites and encouraged more journalists to start their own online news websites.

Many other factors fed the boom of online news sites. In 2005, weekly newspapers were facing financial and political licensing pressures that limited their chances of survival, including the interference of the General Intelligence Department in the appointment of their editors.[12] The Internet was an appealing migration destination for these newspapers. First, the Internet allowed bigger returns on investment given the low development and running cost. Second, it provided a semi-unregulated environment and a safe haven for unchecked slander and defamation.

According to the journalist Mohammad Omar, another factor was the political polarization between two prominent figures in Jordan in 2007, the head of the General Intelligence Department and the head of the Royal royal court. The political battle between these two prominent figures was playing out on online news media sites as journalists propagated the agendas of these two figures. Various news websites exchanged accusations about bribes being taken by journalists on each side.[13]

Just as this open, unregulated nature of the Internet in Jordan pushed media redlines and helped

12 Sa'eda Kilani, "Press Freedoms in Jordan," Euro Mediterranean Human Rights Network, 2002 available at: http://www.euromedrights.org/fra/wp-content/uploads/emhrn-publications/Press-Freedom-in-Jordan-2002.pdf; S. Zaideh, "Licensing of Electronic Websites: Filers and Survival for the Weakest" [in Arabic], 7iber, 2013. http://7iber.com/2013/08/website-licensing/.

13 "The Dahabi List is Out...Where is the List of Awadallah?" Fursan News Feb 3rd, 2012, available at : http://www.forsanalbarlaman.com/newsdetails.aspx?ne=6082 [in Arabic].<Knights of Parliament>

uncover corruption cases, it also made it a fertile environment for financial blackmailing of public figures and private companies. The existence of many news websites, especially those that curate content rather than produce it, made a living for those who hosted blackmailing attempts and threats to publish incorrect and harmful information about the reputations of companies and public officials. This growing unprofessionalism of some online news websites paved the way for officials and parliamentarians to use such unprofessional activities as an excuse to place limits on a pluralistic media environment. They came forward with proposals for government regulation of the Internet that varied in degree from redefining free-speech zones to filtering and censoring content.

V. Formal Control of Digital Expression

Since the online news scene began to flourish as an alternative to the state media in 2007, the state has been continuously attempting to extend the legal framework's jurisdiction over the flow of print content to online content. There are formal techniques that vaguely calculate free zones for online expression. The legislative framework draws these legal free-expression zones first in expanding limitations on speech to online platforms through laws in the Penal Code, the Press and Publication Law, the State Security Court Law, and the Information Systems Crimes Law. In addition to delineating legal free-expression zones, legislative frameworks control the very access to online publishing platforms, through the 2012 amendments to the Press and Publication Law.

Regulating Online Free Speech Zones

The Jordanian constitution protects Jordanian citizens' right to freedom of expression (article 15). It states that every Jordanian shall be free to express his opinion in speech, in writing, or by means of photographic representation and other forms of expression, provided it does not violate the law.[14]

Jordan also has an international obligation to commit to the rights of the International Covenant on Civil and Political Rights (ICCPR) ratified in 1975[15]. Article 19 in the ICCPR asserts the right to access of information and free speech in any medium including the digital sphere. It states:

- Everyone shall have the right to hold opinions without interference.
- Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
- The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
    - For respect of the rights or reputations of others;
    - For the protection of national security or of public order or of public health or morals[16]

While the constitution and ratified international declarations and treaties form the guiding principles for any further detailed legislation, the constitutions allows for exceptions to be regulated in the legislative frameworks. Every citizen has the right to speak within a calculated free-speech block, and anyone violating these blurry lines is subject penalty. Throughout Jordan's history, activists, journalists, and citizens have been charged for voicing oppositional opinions and alleged to have broken the law. These free-speech zones were drawn by the law across all public spheres including media, books, and audio and visual productions and publications. The online sphere was no exception.

1. System of Governance

According to Jordanian law, citizens can be sentenced to one to three years in prison for lèse

14 The Constitution of the Hashemite Kingdom of Jordan, http://www.kinghussein.gov.jo/constitution_jo.html

15 ICCPR signatories and parties, United Nations Treaty Collections available at: https://treaties.un.org/pages/viewdetails.aspx?chapter=4&src=treaty&mtdsg_no=iv-4&lang=en

16 "International Covenant on Civil and Political Rights," Office of the High Commissioner for Human Rights, UN Human Rights, article 19. http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

majesté crimes (Penal Code, 195) and tried in the military-run state security court (Military Court Law, 3.8). The law criminalizes anyone who insults the king or sends a text, audio, or electronic message, or image or caricature of the king in a way that undermines the dignity of his Majesty. The same applies to any messages that insult the queen, the crown prince, guardians of the throne, or a member of a substitution ruling committee.

The Penal Code criminalizes anyone who conducts an activity to subvert the system of governance, or conducts an individual or collective action to change the social or economic structure of the state, or foundational status of the community (article 149).

Jordan has a history of court cases in which these articles have been used to incriminate citizens, especially journalists and activists. The vagueness of the definition of an insult or system of governance grants flexibility in the law's legal interpretation, and thus, flexibility in its application. Individual citizens have been found guilty for voicing critical views about the king, include talking to a colleague (2007), during parliamentary campaigning (2010),[17] and speaking in a barber's shop (2008).[18] However, the numbers of activists detained for these crimes have increased since 2011, the year of the Arab Spring. Between March 2012 and November 2013, at least seventy-one activists were charged in a State Security Court for undermining or opposing the political regime—for chanting or holding signs with anti-monarchy slogans in demonstrations across the country.[19] Most of these individuals were held for voicing oppositional opinions in the offline public sphere. When it comes to the online sphere, because the Jordanian state attempts to maintain its free Internet image, it abstained from officially detaining writers and activists for online speech crimes of lèse majesté or subverting the system of governance. According to human rights lawyer Leen Khayat, the state makes sure to not be explicit about online speech crimes as the reason for detention; however it is mentioned as evidence in court records. The following cases involved citizens and journalists held for such crimes in the State Security Court for content they published online:

- In 2010, university student Emad Al-Ash was tried in State Security Court and sentenced to two years in prison for a lèse majesté crime. Al-Ash was accused of posting a comment in an online forum that insulted the dignity of the king, and triggered ethnic disputes. The police broke into Al-Ash's house and his personal computer.[20]

- The editor in chief of JO24, Alaa al Fazaa, was held in custody for 14 fourteen days for insulting the throne. He was tried in the State Security Court after publishing an article referring to a group on Facebook that calls for Prince Hamzeh, the king's brother, to be the successor instead of Prince Hassan, the oldest son of King Abdullah II.[21]

- In 2012, the journalists Jamal and Sahar al Muhtasib, editors of an online news website, were arrested for undermining the system of governance. They were charged in a State Security Court after publishing an article that made claims about the king's intervention in

17 Christoph Wilcke, "Jordan: A Measure of Reform," *Human Rights Watch*, 8 March 2011, http://www.hrw.org/news/2011/03/08/jordan-measure-reform.

18 Christoph Wilcke, "The Flaws of Jordan's Largest Terrorism Trial," *Human Rights Watch*, 21 November 2011, http://www.hrw.org/news/2011/11/21/flaws-jordan-s-largest-terrorism-trial.

19 Doa Ali and Hussam D'ana, "Undermining Justice: Prosecuting Activists in the State Security Court" 12 November 2013, http://7iber.com/2013/11/martial-secret-and-above-standards-of-justice-prosecuting-activists-before-the-state-security-court/

20 Ahmad Al-shagra, "Jordanian Student Sentenced to Jail for Two Years over IM," *The Next Web*, 19 July 2010, Accessed April 2013, http://thenextweb.com/me/2010/07/19/royal-ash-jordanian-student-sentenced-to-jail-for-2-years-over-im/#!zSL5z

21 "Journalist Alaa Faza Still Under Arrest" [in Arabic], Ain News, 1 June 2010. http://ainnews.net/?p=92906.

covering up a corruption case against a minister.[22]

- In 2013, Ahmad Khdierat was detained in State Security Court for publishing poetry criticizing the king on his Facebook profile. Khdierat was charged with the punishable offense of "lengthening the tongue". [23]

2. Religion

Religious content is regulated through anti-blasphemy provisions across the Penal Code and the Press and Publication Law (PPL). The Penal Code (PC) outlaws any publications that insult individuals' religious feelings or beliefs, and prohibits any individual who publicly insults "divine prophets" (PC, articles 273, 278). While the PC specifies that these crimes can take place in any print publication, map, drawing, or symbol, the PPL addresses issues of blasphemy as well, rendering the applications of these laws vague. The law states that publications are prohibited from publishing any content at odds with the values of Arab and Islamic nations (PPL, article 5). The law also prohibits anyone from publishing libelous or slanderous, defamatory content against religions whose rights are protected in the constitution (PPL, article 38a) or content that insults prophets (article 38b), or content that insults religious feelings or beliefs.

There have been very few court cases filed against journalists and writers for blasphemy in Jordan. For the most part, these cases were against literary work in poetry collections and novels. The low number of cases should be understood both as a result of the state's censorship, and the high level of self-censorship. The Department of Press and Publications has always had the power to pull books from the market under a court order for blasphemy, and it regularly cuts religiously inappropriate scenes from movie screenings.[24] Self-censorship is often practised by journalists as reflected in the 2013 survey of the *State of Media in Jordan*, where 74 to 80 % of Jordanian journalists stated that they avoided reporting on religious issues.[25] The only documented media blasphemy case was held in 2006 against the editors of two weekly newspapers for republishing the Danish anti-Prophet cartoons in an article defending the Prophet. Two editors, Jihad Al Momani and Hashem Khalidi, were charged in a State Security Court.

Court Case against Google

When it comes to the online sphere, there have been no official cases against journalists, activists, or citizens for publishing religiously harmful content online. This set of Jordanian local laws however was used to indict the international search engine Google for providing access to the controversial movie *Innocence of Muslims* in Jordan. In February 2014,, the court of first instance issued an order compelling Google to block links to pages that host the video on YouTube. [26] [27] The lawyer who filed this suit argued that by hosting the video on YouTube, Google violated numerous Jordanian laws

---

22 ***"***Journalist ***F***reed on ***B***ail after ***Twenty-one D***ays in ***C***ustody, ***S***till ***F***aces ***P***rosecution***,"*** Reporters without Borders, 14 May 2012. http://en.rsf.org/jordan-journalist-to-be-tried-before-25-04-2012,42354.html.

23 "State Security Charges Al Khdierat after Publishing a Political Poem" [in Arabic], JO24, 20 December 2013, http://www.jo24.net/index.php?page=article&id=56051.

24 Mlynx Qualey, "Censorship and the Jordanian Reader" *Arabic Literature (in English)*, 4 April 2014. Available at http://arablit.org/2014/04/14/censorship-and-the-jordanian-reader/

25 "The State of Media Freedoms in Jordan (2013)" [in Arabic], Center for Defending Freedom of Journalists, available at **https://tinyurl.com/n5p6mtw**.

26 "Judicial Order Obliges Google to Delete Anti-prophet Film" [in Arabic], *Alghad News*, 19 February 2014. http://www.alghad.com//articles/504291;

27 Mohammad Ghazal, "Google Blocks Access to Anti-Islam Film Trailer in Jordan," *Jordan Times*, 22 September 2012. http://business-humanrights.org/en/google-blocks-access-to-anti-islam-film-trailer-in-jordan

that prohibit insulting the messengers of God identified in the Koran. [28] In an interview he said that the carrier should be held responsible for making the film accessible to people knowing that it carried hate speech. The charges listed against Google in the lawsuit filed in March 2014 included inciting religious hate and racism, insulting Muslims' religious feelings, insulting the Prophet, and defaming Islam.[29]

The gaps in the technical knowledge of what constitutes publishing and hosting content on the Internet were evident in the media coverage of the case as well as the court order. There is still a tendency to deal with the online environment as a physical publishing space where content can be deleted or taken off air. For example, the headline in one of the main newspapers, *Alghad*, stated "Google to Delete Anti-Islam Film." However, the body of the article states that Google has to stop "publishing" and "airing" the anti-Islam film.[30] Although the case is not closed as of the writing of this paper, it represents the possibility of applying Jordanian local law to international companies that host content.

3. Defamation, Libel, and Slander

Jordanian law covers crimes of defamation, libel, and slander across both the PC and PL. The PC provides detailed definitions of what constitutes defamation, libel, and slander. Punishments, however, vary depending on the targeted party. Libeling, slandering, or insulting regular citizens can result in up to three months, six months, or one month in prison respectively. However, one can be sentenced with up to two years in prison for slandering public parties identified as the parliament or one of its members, official institutions, courts, public administrations, the army, or their members on duty (PC, article 191). The same punishment is given for public defamation, slander, libel of a president, ministers, or representatives of a foreign country. People charged with insulting or slandering the king, the queen, the crown prince, or those in line to the throne can be sentenced with up to three years in prison. Insulting a public official can result in up to one year in prison, and up to two years if the official is a judge (articles 193 and 196). Insulting the national flag, symbols, or the flag of the League of Arab Nations can result in up to three years in prison (article 197).

These PC provisions apply to all crimes of libel and slander regardless of the medium through which the crime was committed, which extends it to digital platforms. This is clearly mentioned in a specific provision prohibiting the publication of libel and slander with only a few exceptions (article 198). It allows slander and libel only if it is based on correct information *and* if its publication will benefit the public good without identifying what constitutes these terms. These provisions apply to all offending citizens, including journalists.

The PC covers the legal basis for any crime of defamation, slander, and libel against any citizen. However, its terminology is vague, as are restrictions on speech, and punishment depends on the offenders and the offended. Yet the PPL adds another exclusive provision for slander, libel, and insult crimes against individuals if such crimes are committed through a publication. These provisions are redundant and lend further vagueness to the legal prosecution of crimes of libel and slander in general. The 2012 amendments to the PPL substituted prohibiting slander, libel, and insult against the dignity of individuals and freedoms with prohibiting these crimes against personal individual freedoms, which added a clearer frame for what constitutes these crimes. However, there are still two issues with this provision. First, it can be used for only crimes against individuals and not public officials, which subjects journalists to the vagueness of the PC if they're prosecuted for

28 Interview with Adel Saqf Al Hiet, prosecutor for the Google case.

29 "Court Order Compels Google to Delete Anti-Islam Film" [in Arabic], *Alghad News*, 19 February 2014. http://www.alghad.com//articles/504291.

30 "Judicial Order Obliges Google to Delete Anti-prophet Film" [in Arabic], *Alghad News*, 19 February 2014. http://www.alghad.com//articles/504291.

publishing content about public officials. Second, the definition of insult cannot be applied to a publication because the insult crime defined in the PC needs to take place face to face (PPL, article 38b).In 2010, the proposed cyber crimes law included three more articles to treat defamation in online publications, penalizing sending or posting data or information via the Internet or any information system that involves defamation or contempt or slander, without defining what constitutes those crimes, with a fine of up to 2000 JD (approximately 2800 USD). This amendment was removed after a public uproar.

Between 2010 and 2013 there was an increase in the number of libel and slander cases against news websites in general, according to Press and Publication lawyer Mohammad Qtushiat. While the exact number of libel, defamation, and slander cases cannot be filtered out from the number of cases against all types of media, there were only forty-nine cases against editors and journalists in 2010 compared to one hundred cases during the first nine months of 2013.[31]

4. Public Morals

Jordanian law regulates any activities or speech that offends the public morals without specifying what constitutes these morals across more than one law: Information Systems Crimes Law, the Penal Code, and the Telecommunication law. The Penal Code penalizes any individual who sells, or possesses with an intention of selling or distributing, or prints or reprints any printed obscene material, or drawing, photo, sketch, module, or any other thing that may lead to the corruption of morals. Any individual who participates in these activities or any others, as the law extensively mentions, which involve the public display, distribution, or trade of any of these obscene or morally corrupt materials will be charged and sentenced with up to three years in prison (Penal Code, article 319). However, the Telecommunication law prohibits Internet Service Providers (ISPs) from suspending or blocking Internet or communication services from a client unless the client was using it in an unlawful manner or against public morals. This is reiterated in the ISPs' terms and conditions of service.

The Information Systems Crimes law calls for the detention of up to three months for any individual who intentionally attempts to approach any person under the age of eighteen with sexual material that is published, sent, or produced through information systems or information networks.

According to the director of the Department of Electronic Criminal Investigation, moral crimes were at the forefront of crimes committed online. Because there is no clear legal definition of what constitutes a moral crime, there has been a wide range of cases for the law's application that criminalizes both the alleged abused and abuser. This was reflected in an anecdote mentioned in an interview with cyber crimes lawyer Leen Al Khayat. He described how a lawsuit was filed by an Internet user for being compelled to share obscene images with a fake user account on Facebook. The fake user tricked the target into an online relationship by pretending to be female, and later asked the target to send photos and videos of him in sexual positions. The fake Facebook user widely shared this material online. While the lawsuit was filed by the target against the fake user, the target was also criminalized for creating and sending obscene material.

5. Foreign Countries

The Penal Code penalizes, with up to five years in prison, anyone who conducts actions, speeches, or writings that are unauthorized by the government and that subject the kingdom to hostile acts or that harm relations with foreign countries (article 118). Another article penalizes anyone who insults a foreign country, its military, flag, or national symbol with up to two years in prison (article 122). These articles were used to detain several individuals in 2013. Three Jordanians were charged with

31 Court cases against journalists in Jordan between 2010 and 2013 represented by lawyer Muhammad Qtieshat.

disrupting relations with foreign countries for distributing a sign that supported the Egyptian Muslim Brotherhood. In the online sphere, two cases were documented in 2013:

- In September 2013, Nidal Faraneh and Amjad Maala, respectively the editor-in-chief and owner of Jafra news website, were held in custody in a State Security Court for publishing a video that showed the brother of the Qatar ruler in an inappropriate position with women.[32]

- In November 2013, twenty-three-year-old Ayman Bahrawi was charged for sending a WhatsApp message saying "Sisi is more criminal than Bashar." Bahrawi was charged in a State Security Court for disrupting relations with foreign countries.[33]

6. Supporting Terrorism

Passed in 2006, the anti-terrorism law criminalizes any expression of support for what can be considered terrorism on the Internet. This was reflected through amendments in May 2014 that state:use of information systems, or the information network, or any other publishing or media tool, or establishment of a website to facilitate the conduct of terrorist acts or support terrorist groups, or an organization or a charity that performs acts of terrorism or market[s] its ideas or funds it, or conducts any acts that subject Jordanians or their property to acts of hostility or reprisals.[34]

The danger in this clause is twofold. First, the lack of definition for what constitutes support can extend support to the basic use of symbols and signs, and to sharing content that is considered supportive of terror. Second, the wide definition of what constitutes a terrorist act may subject a larger percentage of the society to this law. The definition includes any act that damages the environment, or disrupts public life. Not only protests will be criminalized under this law, but also sharing a Facebook event that calls for a demonstration could then be considered support of a terrorist group.

While there are no cases prosecuted under these clauses yet, in June 2014 the Jordanian government announced that it would be monitoring Jordanians' comments or announcements that reveal support of ISIS (Islamic State of Iraq and Syria), an alleged terrorist group.[35]

Regulating Access to Online Publishing Platforms

Legislation in Jordan that allows generic censorship of content violates its commitment to the United Nations International Covenant on Civil and Political Rights that it ratified in 1975.[36] In September 2011, the UN Human Rights Committee (HR Committee), a treaty-monitoring body for the ICCPR, issued General Comment No 34 in relation to article 19, which clarifies a number of issues relating to freedom of expression on the Internet. Importantly, it states that:

---

32 "Stopping Nidal Farahneh and Maala Under Investigation," [in Arabic] *Oroba News*, 17 September 2013. Accessed November 2013, http://tinyurl.com/olanh7m

33 "Three Jordanian Activists Jailed for Distributing Flyers Associated with Morsi Supporters," IFEX, 2 October 2013. http://www.ifex.org/jordan/2013/10/02/activists_jailed/.

34 Reem Almasri, "Jordan's Anti-Terrorism Law: A Choice between Security or Speech," 30 April 2014. Available at http://www.7iber.net/2014/04/anti-terrorism-draft-law-a-choice-between-security-or-speech/

35 "Government to Monitor Jordanians' Comments or Announcements Supportive of ISIS, and Threatens to Legally Prosecute Them" [in Arabic], June 2014, Amoun News Agency, http://www.ammonnews.net/article.aspx?articleno=196924

36 International Covenant for Civil and Political Rights—Status of Ratification, Office of the High Commisioner for Human Rights, UN Human Rights, Available at http://indicators.ohchr.org/

- Article 19 of ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and Internet-based modes of expression.

- States parties to the ICCPR must consider the extent to which developments in information technology, such as Internet and mobile-based electronic information dissemination systems, have dramatically changed communication practices around the world. In particular, the legal framework regulating the mass media should take into account the differences between the print and broadcast media and the Internet, while also noting the ways in which media converge.[37]

The state has always tried to find ways to extend the already-restrictive controls on print to the digital sphere. The nature of the unregulated online space in Jordan granted more freedom for online sites to publish content that would not have normally appeared in mainstream newspapers. It also facilitated the creation of a large blogging scene that questioned controversial political issues in Jordan. Since 2007, over 400 electronic news websites raced to publish information about corruption cases and expose public officials and royal family members. The increased Internet penetration rate, along with the increased number of alternative critical news websites and blogs, shifted citizen news sources to the online arena. This rapid decentralization of news and opinions placed more pressure on the government to refer some cases to court to avoid unrest.

The ease of starting a news website has made this online platform a political playground for different adversaries, which in return, increased cases of libel, defamation, and unprofessional journalistic practices. This has solidified the government's reasons for needing official regulation of this uncontrolled space in the absence of a self-regulatory framework. After several attempts to push websites under the publication regulations, the government finally passed amendments to the Press and Publications Law in 2012 to increase its grip on the production of information online. While law attempted to regulate access to online news websites, the Information System Crimes Law of 2010 gave the government the authority, under a court order, to block or shut down systems, networks, or websites that violate content restrictions related to terrorism, prostitution, and public morals.

1. Press and Publication Law

The first incident of the Press and Publication Law being used against a news website was in 2010 in a lawsuit filed by a newspaper's owner against two electronic websites for slander and defamation.[38] The Court of Cassation (Supreme Court) in Jordan issued an order that classified a news website as a publication in accordance with the general definition listed in the Press and Publication Law. This order canceled the first ruling of the Court of First Instance and Court of Appeal to not hold the plaintiffs responsible for what they have published given that the Press and Publication Law does not cover websites. The case was eventually decided in favour of the newspaper owner incriminating the two websites by citing the anti-defamation articles from the Press and Publication Law (articles 5 and 7).[39]

This lawsuit was an alarming development for the future of Jordanian online news. Applying the definition of publications in the Press and Publication Law to news websites meant that all regulations governing publications should also apply. At that stage, many of these articles in the Press and Publication Law contradicted the nature of electronic publishing, therefore making them inapplicable. One example is that the PPL mentions that violating publications are subject to the

37 "Defending Freedom of Expression and Information" (London: Article 19), 9. http://www.article19.org/data/files/Intermediaries_ENGLISH.pdf

38 Eyas Sharaiha, "Websites and the Press and Publication Law," 16 January 2010. Accessed October 2013, http://blog.eyas-sharaiha.com/2010/01/reblogged-websites-the-press-and-publication-law-7iber/.

39 Mustafa Farraj, "Court of Cassation Subjects Electronic Websites to Press and Publication Law" [in Arabic], Accessed October 2013 from http://www.farrajlawyer.com/viewTopic.php?topicId=757.

suspension of their distribution through a court order, which cannot be applied to an electronic website where distribution is the same act as publishing in the online sphere.

Up until 2010, the government could not find a means for blanket regulation of online news production apart from the case-by-case scenarios that were held against newspapers for defamation by MPs. Then in 2011, news websites were officially pushed under the legal umbrella of print publication. The Press and Publication Law was amended to add electronic websites under the definition of print publications and all other provisions in the law were modified to fit the nature of websites, with exceptions for registration or licensing requirements. Parliament declared that this amendment would still protect free online media where, unlike print publications, websites do not have to register as a company in the Chamber of Commerce or get a license from the Department of Press and Publication.[40]

It was the 2012 amendments to the Press and Publication Law that solidified the government's grip over online news spaces in the following forms:

- *Licensing websites*. The law's main amendment included requiring websites to register with the Department of Commerce and obtain a license from the Department of Press and Publication in order to operate, just like any other print publication. All unlicensed websites were set for blocking if they failed to comply with the new registration and licensing requirements. Licensing required that the editor-in-chief be a member of Jordan's Press Association for at least four years for print publications. Any experience in online publications doesn't qualify for the membership period.

- Readers' comments on news pages were considered to be part of the article, and the editor-in-chief and owner were to be held accountable in cases where commentators violated Jordanian law.

- *Blocking as an administrative decision*. The amendments granted the director of the Department of Press and Publication the ability to identify and issue a blocking order for websites that publish news, investigations, articles, or comments that have to do with the internal or external affairs of the kingdom. Classifying a news website depends on the director's judgment under the vague definition listed by the law.

Elastic Definitions, Elastic Application: Blocking a Blog

Lawyers reviewing the developments warned that the inability to define what constitutes a news website in the online sphere extended the reach of the law to any website or page that publishes content about Jordan, including social media pages and blogs.[41] In June 2013, 300 websites were blocked as a result. Of the blocked websites, two were video production houses, one producing features on political and social issues (Aramram.com), and the other providing broadcasting for live debates, talks, and demonstrations (Jordandays.tv).

Despite assurances from the senate about keeping social media websites and blogs out of this law's reach, 7iber Dot Com (a blog at the time), was blocked a month after the initial blocking order. Definitions for what constitutes a blog and a social website were not officially or legally specified. Identifying a website as news relied on the single judgment of the director of the Press and Publication Department. In an interview with the director to investigate the legal process through which 7iber was blocked, the director mentioned that 7iber, although not a news website, publishes

40 "National Direction Committee approves Press Law with the collaboration of Jordan Press Union" [in Arabic], Jerasa News, 2011, Accessed 12 October 2013, www.gerasanews.com/print.php?id=53035.

41 M Qutaishat, "Legal Review of Press and Publication Law" [in Arabic], *Ammannet*, August 2013 ar.ammannet.net/news/169716.

political analysis, which made it qualify as an electronic site and thus subject to blocking. The director said that a blog is a private personal page that requires authorized access.[42] Although 7iber qualified under the law, according to the director, it could not comply with licensing requirements set by the law because its editor-in-chief does not have a four-year membership in the Jordan Press Association.

The 7iber blocking case revealed the scope of web pages the law intended to cover despite the official rhetoric on targeting news websites. The law was designed to control any political online space that publishes news or analysis on Jordan. Any website selected by the Press and Publication Department's director, without due process, as falling under the loose definition of an electronic website must fulfill the registration and licensing requirements in order for users in Jordan to access it. This loose definition can also include international news agencies that report on Jordan. However, the law was applied to only websites identified as Jordanian. The law offers more flexible registration requirements for specialized publications or websites without giving a concrete definition of what constitutes such specialized venues. According to the director, specialized websites are simply those that do not publish any political content about Jordan, but stick to specialized topics like sports, parliamentary, and social issues.

The Information and Communication Association of Jordan (Intaj), an NGO representing the ICT business, made it clear through various correspondence to the ministry that amendments to the law and its loose definitions will negatively affect investments in the ICT sector. First, the law has discouraged Google from opening an office in Jordan because of the unclear legal definition and application that allows the law to reach international platforms with public pages like Facebook and Twitter. Second, the law has also harmed the local hosting business in Jordan because websites that were locally hosted were blocked across the entire world, while those hosted abroad were blocked only in Jordan.[43]

The response from the Director director of the Press and Publications Department repeated the assurance that this law would not affect the ICT sector and businesses. It continued to reflect a lack of technical awareness of the functionality of web platforms. It repeated the misconception that the law will not reach social media platforms, even if they publish news about Jordan, because they require a user account for access.[44]

Executing Formal Blocking Requests: Legislative Gaps

The following actors were involved in blocking websites in June 2013: the Press and Publication Department (DPP), the Telecommunication Regulatory Commission (TRC), and the ISPs. After the ninety-day grace period given to websites to correct their status, the director of DPP requested a blocking order for selected unlicensed websites. This order was in turn sent to the executive entity of the Ministry of Information and Communication Technology (MoICT), the TRC, which requested all ISPs to filter the listed websites. As mentioned, the Press and Publication Law grants the DPP director the authority to order the blocking of any unlicensed websites that match, according to his personal judgment, the definition of a news website. While the act of ordering the website blocking was legally framed through the law, the execution of the order through the TRC did not have legislative coverage. Although executing a blocking order through ISPs is not listed among the official responsibilities of the TRC in the Telecommunication Law, the ISPs nevertheless complied with the blocking order.

---

42 L. Ejielat, "No to Government General Custody" [in Arabic], 7iber Dot Com, 3 July 2013, http://7iber.com/2013/07/what-is-a-blog/

43 Intaj Letter to the Head of Press and Publication Department [in Arabic], 7iber, 11 July 2013, http://7iber.com/2013/07/intaj-letter-on-website-censorship/; Interview with Abed Shamlawi.

44 "Censorship Blocks Trust and Investment: Intaj's Response to Shawabkeh" [in Arabic], 7iber Dot Com, 24 July 2013, http://7iber.com/2013/07/intaj-shawabkeh/

Legal gaps in execution also unfolded in the lawsuit that 7iber filed and lost against the official blocking order. The Higher Court of Justice dismissed the case because 7iber's blocking order came through an unofficial email and was not listed in the initial official blocking order. The court was able to consider only the first printed and signed blocking order as official. Since 7iber was not listed in the first official order, the court inferred that this meant 7iber was not technically blocked. Despite the court decision, for ISPs the blocking order in the form of an email was official enough to execute it. The administrative blocking requests could not be tracked given the lack of an appeal system for orders coming from the Press and Publication Department.

The license agreement between the TRC and the ISPs states that the licensee should collaborate at all times with the TRC or their authorized representatives in practising the assigned functions of the TRC listed in the Telecommunication Law. However, TRC's functions in the Telecommunication Law do not refer to ISPs executing content-blocking orders on the Internet. This function was included in the proposed amendments to the Telecommunication Law that preceded the passing of the new PPL, but the amendments remained in draft status during the blocking order.

This was not the first time that ISPs responded to government blocking requests without a legal framework specifying the execution. Prior to 2013, official requests to censor content by the ISPs were almost non-existent. There is one recorded case in 2001 when the government asked ISPs to block access to the US-based newspaper, the *Arab Times*. The newspaper published controversial and inflammatory articles on Jordan's monarchy and government.[45]

2. Information Systems Crimes Law

Passed in 2010, the Information System Crimes Law was set to regulate crimes of online fraud, identity theft, and underage sexual abuse committed in cyberspace. It also regulates illegal access to websites and information systems without defining what legal access is. In addition to criminalizing hacking into online financial systems, the law penalizes users who:intentionally use the network or any information system to promote prostitution with up to six months in prison and a fine of up to 5000 JD ($7050 USD) (article 9).use any information system within a/the network to facilitate terrorist activities, give support to a group or an organization that conducts terrorist activities, or promote its ideologies (article 10).intentionally enter, without a permit, or in violation of, or exceeding authorization, an electronic website or any information system, by any means, to see data or information that is not available to the public, affecting national security, foreign relations of the kingdom, public safety or the national economy; the user shall be punished by imprisonment for no less than four months and a fine of no more than (5000) five thousand JD (article 11).

Apart from the loose definitions of access and entry to websites, the law also grants the court the authority to request to block or take down a website or an information system if it is used to violate any of the provisions in the law.

45 *Arab Times* continues to be the Only Blocked News Website in the Kingdom, Media Sustainability Index Report (2009), IREX. Available at : http://www.med-media.eu/wp-content/uploads/2014/07/MSIMENA09_Jordan.pdf

VI. Informal Jurisdiction on Digital Expression

Unlike formal methods of censorship, informal techniques for exercising control over access to and production of digital content exist outside the official legislative framework that is embodied in Jordanian law. Informal control is executed by different state and private entities through internal regulations that are not subject to public scrutiny or discussion. These entities are the General Intelligence Department, the Ministry of the Interior, the ICT departments of public universities and ministries, and ISPs.

Jurisdiction of the General Intelligence Department

The Jordanian security apparatus has a long history of intervening in the media scene through formal and informal means: threatening or incentivizing journalists, banning books, and approving senior editors-in-chief. An intelligence officer is also placed at each newspaper's printing house, according to one weekly magazine editor who was surprised to know that the printing of the magazine was halted for having an article written by an oppositional figure.[46] In 2011, hundreds of journalists led a demonstration demanding an end to the security apparatus meddling in their work. This intervention was also publicly criticized by the previous minister of information in a 2012 conference on freedom of expression in Jordan.[47]

With the decentralization of media production through the growth of online news websites and the blogging scene, the security agencies were no longer able to control production of information prior to publication. Many of the online spaces did not have a physical office or an identified editor to be reached, and many political bloggers concealed their identity. Before 2010, the online sphere did not have a legal framework to regulate its content. These factors gave news websites a relatively free space to reveal corruption cases and publish leaked incriminating documents about public officials and members of the royal family. According to journalists, intelligence-gatherers resorted to removal requests after publication and "friendly" threatening phone calls. Journalists reported several cases where editors complied with intelligence department requests and removed selected articles from their websites. One example was the removal of a translated Wikileaks document in 2011 upon request for fear of inciting conflict. The Wikileaks document reported the controversy around the official order to replace the picture of the late King Hussein with Prince Hussein, the successor to the throne, in all public institutions. Another way intelligence seekers adapted their media penetration techniques was by developing groups of journalist friends through financial incentives. While evidence remains anecdotal, these incentives were reported by the surveyed journalists responding to the 2013 survey on the state of media in Jordan.[48] Journalists reported that at least 70% of websites accepted bribes and payment for investigative content.

Intervention in content production does not stop at interfering with journalists—it extends to bloggers, regular users, and activists. Several bloggers, who asked to remain anonymous, reported being called in by the intelligence department for an "introduction party." One blogger, Mohammad Omar, publicly announced being called in for a meeting at intelligence headquarters in March 2011 about his critical writing. According to him, the intelligence department wanted to deliver the "we are watching you" message.[49] Five hours after publishing an article criticizing the king's performance in

---

46 S. Zaydeh, "Security Apparatus: Crossing Squares...Restricting Freedoms" [in Arabic], Ammannet—Human Rights Documentaries. 4 August 2011, http://ar.ammannet.net/documentary/news/456/

47 "Majali Criticizes the Intervention of Royal Court and Intelligence in Jordanian Media" [in Arabic], Assawsanah News, 2 February 2012, http://assawsana.com/portal/pages.php?newsid=62831

48 "The State of Media Freedoms in Jordan (2013)" [in Arabic], Center for Defending Freedom of Journalists, available at **https://tinyurl.com/n5p6mtw**.

49 "Blogger and Journalist Mohammad Omar: The Call from Intelligence Was to Deliver a Message" [in

2012 on a multiuser blog, the blog was hacked and the post was moved to the WordPress trash bin, according to the blog administrator (who desires to stay anonymous).

In 2007, a blogger who writes under a pseudonym was asked to leave a Jordanian blogs aggregator by the aggregator administrator who was under pressure from Intelligence to identify the people behind the blogs. Not wanting to disclose such information, the administrator asked the blogger to leave the aggregator to avoid further Intelligence pressure, but eventually ended up closing down the aggregator.

These intimidation techniques do not have a documented life of their own because they remain anecdotal and are sometimes never spoken about. They were mentioned during the focus groups conducted by our research team's exploration of issues in university students' accounts. Across two focus groups in Irbid and Karak, there were six anecdotal stories about students and professors who were called in by Intelligence for posting content or comments against the king or the regime.

To maintain the image of Jordan as a country that offers relative freedom of expression, these intelligence department interventions remain under the radar because they take place frequently at an individual and unsystematic level, according to human rights Lawyer Leen Khayyat. These techniques, and the criminalization of journalists and activists under the State Security Court, have led to the most effective, yet informal type of censorship: self-censorship. In the 2013 report on media freedom in Jordan, 84% of surveyed journalists reported practising self-censorship on different topics. Journalists reported avoiding the following taboos (in order): Jordan's armed forces, the judiciary system, religious issues, security services, sexual issues, and criticism of Arab and foreign heads of the state.[50] Journalists' sentiments about censorship are mirrored in respondents' answers to the Perceptions of Online Monitoring in Jordan surveys and focus groups discussions with young Jordanians (see Appendix 1). While the participating sample is unrepresentative of the Jordanian online population, answers coincided with the general self-censorship practices of the country's journalists. In one of the surveys, respondents reported a strong feeling of surveillance: 73% believed that there are official entities collecting and storing their personal information and online interactions. While this question ("Do you believe that official entities are collecting and storing your personal information and interactions online?") was asked on its own, it reaffirmed the answers to another question on the extent to which participants perceive different types of monitoring online: official entities, employers, friends and family, and different online groups. Participants believed the following entities practise online monitoring in order: official monitoring (71%), employers' monitoring at the workplace (61%), monitoring of different user groups (48%), and the monitoring of friends and family (41%).

The research team understands the limitation in the collected data, given the unscientific sample; however, students from focus groups have also reported a similar sentiment with a more in-depth perspective. Across two focus groups in Irbid and Karak, there were six anecdotal stories about students and professors who were called in by the intelligence department for posting content or comments against the king or the regime. The royal family and the military were the two topics that students from focus groups mainly avoided in their online interactions on Facebook and Twitter. One student stated that, "although many of my friends criticize the royal family, I try not to cross that line, because I fear for my future." Few students mentioned that the Arab Spring redefined the boundaries of what criticism is possible: you can criticize the royal family if you do it "respectfully," citing an example of a demonstration that threatened the regime, not the government. Participants felt that offline criticism of the king within a crowd is safer than individual criticism online.

Arabic], Skeyes News, 6 March 2011, Accessed 6 May 2013, http://skeyes.wordpress.com/2011/03/16/6546513213241654/.

50 N. Abdul Hadi, "Obvious Setback in Media Freedoms Violations in 2013 in Jordan" [in Arabic], May 2014, Ammon News, http://tinyurl.com/qjbt5vp

Bringing all these findings together from journalists, online users, and focus groups indicates that self-censorship is a much more powerful form of expression control than the formal legislative tools. Their content filtering takes place on an individual level where most citizens are careful to stay within a safe zone—sometimes a zone tighter than what the formal legislative control requires.

Jurisdiction of the Ministry of Interior

In 2006, Jordan entered the *Guinness World Book of Records* for having the longest street of Internet cafes in the world: 130 cafes on a 300-meter-long street in the city of Irbid.[51] The huge rise in the number of Internet cafes, which gave greater Internet access for Jordanians, incited the Ministry of the Interior to publish a regulation strategy to organize this scene. Issued in 2008, the strategy ordered Internet cafes to provide the necessary measures to monitor users and block access to pornographic content. In 2010, these instructions were modified to include the following conditions in orderneeded to receive an Internet cafe license: [52]installing surveillance cameras at the doors of Internet cafes with a capacity to retain recorded data for up to three months;providing a main server that records accessed websites, time of access, and the IP address of the node through which it was accessed (the server should save this information for up to six months);keeping a daily record of users' national IDs, node number, and time of usage;taking the necessary steps to block access to any visual or auditory material that promotes prostitution; harms religious beliefs or the ruling party; incites racism; or promotes the abuse of drugs, tobacco, medicine; gambling websites; or websites that demonstrate the illegal making of special material for military purposes.

These instructions contradict the constitutional right of protecting citizens' private communications in accordance with Jordanian legislation (article 18). These regulations however gave the Ministry of the Interior the authority to control access to Internet websites through private access points such as Internet cafes.

It is difficult to determine exactly how these instructions affected the operation of Internet cafes, given the different variables affecting the Internet access scene in Jordan. The number of Internet cafes in Irbid dropped to less than a dozen compared to 130 in 2006. The 2012 "National ICT Usage at Home" survey reported a drop in the percentage of users accessing the Internet from 12.1 to 6% between 2010 and 2013.[53] In interviews, owners of the remaining cafes attributed the closing down of the cafes to the increased access of home and mobile Internet, the financial and logistical burden that these new requirements impose, and users refusing to give out their personal information (in this order). While the drop in the use of Internet cafes cannot be directly attributed to increased monitoring in these cafes, Internet cafes were ranked the least secure by participants in the online survey about the level of perceived security when using the Internet across different locations (Appendix 1). Between home, work, university, and Internet cafes, Internet cafes and universities were where participants felt the least secure while browsing the network. Forty-six percent of respondents said they do not feel any kind of security in Internet cafes, and 40% feel the same about university networks. The home got the highest rate of support (44%) as the location where participants felt absolute security online. Logging in from work, or the mobile got the highest percentages (46%) of people feeling somewhat secure.

---

51 "The Day Jordan's Internet Went Dark" *Jordan Business*, October 2012, http://www.jordanbusinessmagazine.com/cover_story/day-jordan%E2%80%99s-internet-went-dark

52 "Amended Instructions to Regulate the Work and License of Internet Cafes and Centres" [in Arabic], Al Dustour, 3 June 2010, Accessed 14 May 2013. http://tinyurl.com/pc67owz.

53 National Survey on Technology Usage in Households, Department of Statistics 2013,Department of Statistics, ICT Usage Survey 2013, Distribution of Internet User according to the Location of Access, available athttp://www.dos.gov.jo/owa-user/owa/techno.show_tables1?lang=A&year1=2013&t_no=36

Cafe owners stated that at the beginning of the Arab Spring, the Criminal Investigation Department (CID) was keen on maintaining regular collection of user data, and then slowly changed to an upon-request data collection strategy. Different anecdotal stories were cited by owners about CID requests to investigate the online activities of clients without warrants (which should be granted by the Ministry of the Interior). Requests from the CID increased during the times of demonstration and political unrest in March 2011. An Internet cafe owner in Irbid mentioned that during these times, the CID requested information on many users who used to engage in anti-regime discussions. A focus group participant from the city of Karak mentioned a similar story:An engineering student had a strong oppositional online voice against the regime on forums and social media websites. One time the CID stormed all Internet cafes in the area to collect personal information on all users who used the Internet around that time to find that particular person. The CID closed down our place for a week when they found out that our cafe didn't collect users' personal data. Then they discovered that he was logging in from the engineering department network at the university and were able get him.[54]

The enforcement of these instructions varied in intensity according to Internet cafe owners, which is reflected in the variation of compliance across cafes. All Internet cafes surveyed had cameras, but only some collected identification from users. One owner of a cafe mentioned providing weekly camera records to the CID. When it comes to accessing websites, all Internet cafes filtered pornographic content. Some denied access to websites such as the Forum for Religion-Disaffiliated Arabs, a forum that questions religions and beliefs in the Arab world.

Instructions from the Ministry of the Interior pushed Internet cafes to practise an additional role in controlling access to online content and blocking websites on their network if they were deemed to violate the regulations. Although unconstitutional, the regulations placed on Internet cafes continue to push the private sector to a larger role in designing the online user experience, and controlling access to online content rather than sticking to their role as neutral providers of the service.

Internet Service Providers' Jurisdiction

De-facto Censorship: Responding to the Press and Publication Department's order to block 300 websites in June 2013 was not the first time ISPs practiced censorship. In January 2011, and before the amendments to the Press and Publication Law, Orange (the main telecom company) blocked a satirical blog criticizing the Jordanian regime under a provocative name without a formal blocking order. Unlike the case of the *Arab Times* website in early 2000, the Orange decision to block was not backed by an official governmental request.

Suspension of Internet Service: ISPs' authority to regulate access to online content stems from not only their ability to block access to certain pages, but also to suspend the communication medium entirely.

Although the telecommunication law prohibits ISPs from suspending or cancelling services, there are exceptions. According to the telecommunication law, ISPS have the authority to suspend or stop the service if the usage of the service violates the running legislations or public morals (article 58).[55] These suspensions do not require a court order; they leave the identification of violations to the ISPs' own interpretations.

More details on the proper usage of the service can be found in the terms and conditions of service on the back of any broadband Internet contract. Across all terms and conditions, criteria of acceptable usage starts with the official language for the widely defined conditions in the

54 The participant requests anonymity.

55 Telecommunication Law (article 58), [in Arbic], Legislative and Opinion Bureau. Available at **http://tinyurl.com/p8mpseo**.

telecommunication law. For example, most ISPs state their authority to completely stop the customer's service for security and public safety needs, or if the user attempts to use the network for fraud or in a way that harms public morals, using the criteria from the telecommunication law. However, some ISPs extend the blanket of violations that can lead to service suspension without a court order: sending, receiving, uploading, or/and downloading, or/and using or/and reusing material which is abusive, indecent, obscene, menacing, or in breach of any copyright, confidence, privacy, or any other rights; and sending or procuring the sending of any unsolicited or promotional material.[56]

These conditions follow the trend in the telecommunication law by using either loosely defined terms such as "public morals" or extending restrictions on usage with vague and restrictive terms. The lack of an official, precise definition of a violation leaves the ISPs with the ability to determine what constitutes a violation without a legislative framework detailing cases of suspension.

Data Hosting: Most telecom companies in Jordan provide web-hosting services for websites. These services are governed by certain conditions in the contract that give the hosting companies the ability to terminate or disconnect service for any illegal or improper purposes, including, but not limited to, fraud, infringement of copyright, or harassment.[57] These conditions do not necessarily imply that termination can take place as a response to due process or a court order, and do not specify the terminology of what illegal or improper use is, which again leaves it open to interpretation.

For example, Orange Telecom has the ability to terminate service with one week's notice in case of a breach: "

Any breach by the customer of any of its obligations hereunder shall render him or her liable for termination or temporary disconnection of the service, provided that the customer was given a notice one week in advance and did not correct the alleged breach."

Given these conditions, websites that are found in violation have a high risk of being globally blocked for the suspension of their hosting service.

Jurisdiction over Public Internet Networks

Public University Networks: The 2013 Internet Usage Survey reported that 11% of Jordanians access the Internet through universities, compared to 18% in 2010.[58] All Jordanian universities have Internet policies for their networks. These policies range from guidelines for secure, efficient usage of the network to prohibiting usage and access to certain websites. In its Internet policy, the Jordan University for Technology and Science (JUST) explicitly indicates that it uses filtering software to block access to immoral content or "nonuseful" websites. It also prohibits students from using chat services, and popular online forums unless it is for strictly academic purposes, and only if the student uses his or her real identity. The university can suspend any student's access for technical or security reasons without prior notification or proof of violation.

While some universities attempt in their policies to be reactive to violations and threats of usage, other universities allow very limited usage of their networks. An example is Mutah University, a public university that allows access to only web pages that belong to the university on its network.

---

56 Umniah, ADSL Terms and Conditions, 2013.

57 Orange, Hosting Terms and Conditions, 2013.

58 National Survey on Technology Usage in Households, Department of Statistics 2013,Department of Statistics, ICT Usage Survey 2013, Distribution of Internet User according to the Location of Access, available athttp://www.dos.gov.jo/owa-user/owa/techno.show_tables1?lang=A&year1=2013&t_no=36

In an online survey investigating university Internet network policies and student perceptions (appendix 2), most respondents across a combination of six public and private universities reported that their universities block access to certain websites. Students who reported censorship on their university network mentioned blocked access to pornographic websites, social networks, and filtering tools that often deny access to innocuous websites. When it comes to monitoring usage, a few respondents mentioned being asked to close the websites they were surfing, including email websites and YouTube. This usually happened after receiving a direct exhortation from a lab supervisor. The mentioned Internet policies and students' perceptions reflect only one part of the universities' role in censorship—they are evidence of the scope of limitations that universities exert on their students' Internet experience. Some public universities still think of the openness of the Internet, and the use of online forums and social media websites, as a threat to academic research. Other universities think of it as a threat to security, which pushes them to intensify surveillance and monitoring of students' usage.

Government Ministry Networks: When it comes to content control, the MoICT has the authority to ban websites on the national network through regulations issued by the Strategic Policies Unit of the MoICT. For example, pornographic websites are banned across the government network, legislated through the Strategic Policies Unit. Each government institution has the authority to request a website ban on its own network, such as blocking Facebook on the MoICT Intranet and the Ministry of Education network for a temporary period in 2011.

In 2010, the Minister of Information Technology ordered online news websites blocked on the government network. After conducting a study that claimed that surfing one hour of news a day by one government employee around 70 million JD (100 million USD) per year in wasted time, this decision was taken to ostensibly improve the efficiency of the public service. It was revoked a year later.[59]

Jurisdiction on Domain Names

At the time of writing, there were 125 domain names with the . الأردن extension and 4400 domains with the .jo extension.[60] The National Information and Technology Center (NITC), the semi-government centre, is the exclusive registry and registrar[61] for the top-level domains (TLD) (.jo), (.الأردن), and all other second-level domains (SLDs). This means that an approval from the NITC's director of e-operations is required for a .jo DNS to be registered. For a fee, several ISPs offer the service of applying for a domain name, but they act as mediators and not registrars because the approval still has to come from the NITC.

The NITC adapted the international standard requirements of registration to the country's local context as mentioned on their website. The domain name registration follows a non-open policy through which the registrant needs to show sufficient documents. Any registrant of the (.jo) or (.الأردن) needs to be an entity residing or operating with a formal registration or approval. Exceptions are given to educational and not-for-profit projects or organizations. For example, a commercial entity or network needs to submit its registration license issued by the Ministry of Industry and Trade, and a political party needs to provide their Party Approval documents, and a letter needs to be issued by the head of a family or tribe for DNSs of family names. No domain names can be provided for non-registered entities. Jordanian citizens can register domain names only under (per.jo).

---

59 "Jumaa: Employees Spending One Hour on the Internet on Daily Basis Costs the Government 70 Million Dinar Yearly" [in Arabic], *Ammon News*, 8 May 2010, accessed June 2013. http://www.ammonnews.net/article.aspx?articleNO=66529.

60 "Domain Names Service conditions," https://www.dns.jo/statistics.aspx.

61 "Information for Registrars and Registrants" ICANN available at: https://www.icann.org/resources/pages/registrars-0d-2012-02-25-en

As for the domain names content, the NITC practises more control by adding a list of prohibited domain names with vague specifications. For example, a domain name is prohibited if it violates Jordanian laws, social norms in Jordan, or has false language and bad terms. The terms listed are extremely vague with no definitions or standards, which makes the decision of domain name approval subject to personal judgment and political inclinations. The director of security at the NITC mentioned that websites that may harm the reputation of Jordan will not be given a .jo domain.[62]

While the process and requirements of a .jo DNS application may seem to be a deterrent for registration, the cost of DNS registration is the main issue behind the low number of businesses registering under .jo. First-time registration fees for a .jo domain cost $141 USD with a $71 USD renewal rate.[63]

62 Interview with Yousef Sarayrah, director of security at the National Information and Technology Center, April 2013.

63 See "General Payment Issues," https://www.dns.jo/paymentIssues.aspx.

VII. ISPs Technical Jurisdiction

We identified the formal and informal forces that control the consumption and production of digital information. These factors were identified by mapping visible legislations and less visible ones: internal policies, terms of service, news, and anecdotal accounts from media organizations and journalists. On top of creating a comprehensive narrative of scattered information controls, this research also attempted to explore the invisible technical aspect of censorship. While Press and Publication Department requests to block websites are not always visible to the public, the ISPs' application of these orders are never visible or transparent. The technicalities of blocking, and realities of how ISPs apply the order, are another layer of informal control, or what we call the informal of the formal. To free themselves from legal liability, ISPs filter content based on blocking orders by the Department of Press and Publication. However, the invisibility of blocking, and the level of complexity used for blocking or filtering content, adds another level of informal censorship and prevents users from access to content.

The research team partnered with the Citizen Lab to perform network measurements to identify trends in ISPs blocking that took place in June 2013.

Methodology

To test Internet filtering in Jordan we used a set of network measurement tools and techniques the Citizen Lab has developed as part of the OpenNet Initiative. The tests rely on software written in Python in a client-server model, which is distributed to researchers. The client program is run from a computer from a network within a country of interest. It attempts to access a pre-defined list of URLs from a network in that country (the field) and in a control network (the lab). In our tests, the lab connection was the University of Toronto network, which does not filter the type of content we test for. Once the tests have been completed, the results are compressed and transferred to a server for analysis. A number of data points are collected for each URL access attempt: HTTP headers and status code, IP address, page body, and in some cases, trace routes and packet captures. A combined process of automated and manual analysis attempts to identify differences in the results returned between the field and lab and isolate instances of filtering.[64]

A sample of 182 URLs was curated from blocking orders and media reports. We tested this URL list on three broadband services offered by different ISPs in Jordan:

Orange, Mada, Zain, and Umniah. All of the URLs tested were websites of Jordanian news organizations that had been reported as blocked or at risk of being blocked. Since this was a very focused testing sample, we cannot extrapolate from these results the proportion of sites blocked in general or what other types of content may be blocked.

Results

In June 2013, all ISPs applied the blocking orders but with variations in the number of blocked websites and blocking techniques. We found that Orange blocked 113 URLs, Mada blocked 90 URLs, Zain Jo blocked 75 URLs, and 35 URLs were blocked on the ISP Umniah. Differences in the number of blocked websites across ISPs result from the lack of a process by the Press and Publication Department to ensure the application of its blocking order.

Technical tests in June 2013 showed that ISPs used three techniques for filtering: DNS tampering, TCP reset, and entirely blocking the website server (appendix 3):

64

For details about this process, see Masashi Crete Nishihata, Ronald R. Deibert, and Adam Senft, "Not by Technical Means Alone: The Multidisciplinary Challenge of Studying Information Controls," Social Science Research Network, 16 May 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2265644

- Most ISPs used DNS tampering to block most websites which is often the easiest censorship method to circumvent because users can configure their computers to use an alternative DNS service or access websites directly by IP address.

- Mada used multiple techniques to filter. In addition to DNS tampering, Mada entirely blocked three IP addresses to prevent any traffic from reaching the censored website server. With this method, the use of an alternative DNS service to circumvent DNS tampering would not be effective if all traffic between the client and censored server is blocked. This technique was also used by Umniah.

- Zain Jo used TCP reset packet injection to block seventy-five websites. In this method of censorship, a middlebox (a device located between the user and the censored webserver) injects a fraudulent reset packet signalling both the client and server to sever the connection. This is a less common method of censorship because it is more technically intensive than most other methods. This method cannot be circumvented by changing DNS settings.

These results show variations in the application of formal blocking requests by ISPs. While reasons behind these variations are not confirmed, they reflect the underlying extent to which ISPs are participating in applying further controls beyond the required blocking orders. Blocking URLs will relieve ISPs from their legal liability but there is nothing that specifies the blocking techniques. The choice over which blocking technique to use could reflect both ISPs' blocking mentality, and the available technologies and equipment in the ISPs network that could stand between the user and the website that s/he attempts to access. Therefore, choosing to apply DNS tampering is choosing a way to relieve the ISP from legal liability but it also leaves space for users to embark on different features of the Internet that allow them to access any content. On the other hand, using a more complex technique, like TCP reset, indicates the sophisticated equipment used by the ISP to gain full possible control for monitoring traffic and accessing data.

VIII. Perceptions of Online Monitoring in Jordan

The first parts of this paper outlined the formal and informal forces of control over content production and consumption. Evidence of these forces was collected through legislative analysis, court cases, anecdotal first-hand experiences, and analysis of internal policies and terms of service. Here, we explore trends in how these formal and informal controls are affecting Internet use in Jordan, generally, and in universities specifically. These surveys aimed to explore how the perceptions of these formal and informal controls are changing user behaviour online, and their efforts to access information in a censored digital environment.

Two surveys (see appendix 1 and 2) testing perceptions of privacy and surveillance for online users ran online for a period of six weeks (from 13 March to 28 April 2013). One survey targeted the general online user, while the other targeted university students. Although these two surveys were not representative of the entire online user population nor the student population in Jordan, they aimed to highlight emerging trends in the informal restrictions on online speech, and open up further opportunities for national-wide surveys on such issues.

Sample Background

The first survey explored perceptions of online surveillance and how it changes users' online behaviour when accessing or creating content. It was published on 7iber and distributed through 7iber's social media (Facebook, Twitter) networks. During the period it ran, eighty-three answers were submitted. While there is no evidence to confirm respondents' residency, only 15% reported not residing in Jordan. The reported residency does not affect the reported perceptions. Most participants were between the ages of twenty-one and forty (89%), and the majority were men (65%), from the capital Amman. The second survey was distributed through students' networks and mailing lists, in addition to the social networks of the Jordan Open Source Association. The survey received around70 responses indicating that participants were between the ages of eighteen and twenty-two years old.

Findings

The surveys did not seek to represent the entire Jordanian online community or Jordanian students in universities. However, responses from online users have corresponded with the previously defined formal and informal forces that had an influence on their online behaviors. We noted the following trends in respondent answers:

- **Perceptions of informal monitoring is affecting users' behaviour online and translating into self-censorship.**

  There is a strong feeling of being monitored among respondents to both surveys. The majority of the online population (73%) believed that there are official entities collecting and storing their personal information and online interactions. While this question was asked on its own ("Do you believe that official entities are collecting and storing your personal information and interactions online?"), its answers corresponded to the answers to another question about participants' perceptions of the availability of monitoring done by official entities, employers, friends and family, and different online groups. Participants believed the following entities practise online monitoring in order: official monitoring (71%), employers' monitoring at the workplace (61%), monitoring of different user groups (48%), and the monitoring of friends and family (41%).

- **The extent to which participants' perceptions of monitoring affect their interactions online was different according to the monitoring type.**

  Official monitoring seems to have the most influence on respondents' online interactions because 50% believed that it has a big influence on their interactions. Other types of monitoring were either "slightly affecting" or do not have any effect for most participants. Friends and family monitoring (41%), and employers (38%) had the biggest share in the types of monitoring that slightly affected

participants' online interactions. Perhaps one way to gauge how participants' interactions are affected by such perceptions of monitoring is that 75% reported self-censorship on social media websites.

- **When it comes to access and usage behaviours of students in universities, almost all of the responding students affirm that university networks blocks access to specific websites.**

  Students explained in open-ended questions that universities do not allow access to pornographic or harmful websites, but students also confirm that several universities block access to social networks and their filtering tools often deny access to "innocuous" websites. In several distinct cases, some students mentioned that they were asked to close the websites they were surfing, including email and YouTube. This happened after receiving a direct exhortation from a lab supervisor. Non-technical censorship was also performed in some universities—students were intimidated if they expressed opinions in disfavour of the university or specific instructors. It is relevant to mention that several universities neither censor nor block any web content and apparently did not adopt any filtering mechanism.

- **While formal legislative controls and informal usage policies are the most visible, very few Internet users are aware of Internet laws and policies that regulate their access to online content.**

  Although 78% of Internet user respondents do not believe that online content should be regulated by official entities, their awareness of such laws is generally low. Participants were asked to report on their level of awareness of laws and policies that regulate online content, specifically: the Press and Publication Law, the proposed draft of the Telecommunication Law, Cyber Crimes law, and their Internet's connection terms of agreement. Those who were not aware of any of these laws constituted the highest percentage. When it comes to being slightly aware, the Press and Publication Law took the highest percentage. In relative terms, there is better awareness (slightly aware) among respondents of the Media and Publication Law, and telecommunication law compared to the Cyber Crime Law and ISPs' terms of agreement. Among student respondents, almost half reported that no specific Internet use policies exist in their universities, and even if they do exist, most believe they were not easily visible or publicly available. Fourteen percent of students reported they are not able to connect to the university network with their own device; when this is allowed, 30% are required to obtain credentials in order to connect.

- **Informal information controls applied in Internet cafes and university network access have become less appealing to users. The most common locations through which online users access the Internet are locations perceived as mostly secure: home and work.**

  According to the ICT Usage Survey 2013, most Jordanians access the Internet from their homes (89%), work (13%), schools (13%), universities (11%), and Internet cafes (5.9%). Online surveys attempted to evaluate how their sense of security online changes according to where participants access the network. Between home, work, university, and Internet cafes, participants felt the least secure while browsing the network from Internet cafes and universities. Of the respondents, 46 did not feel any kind of security in Internet cafes, and 40% feel the same about university networks. Their own homes got the highest ratings (44%) for where participants felt absolute security online. Logging in from work, or the mobile got the highest percentages (46%) when it comes to feeling somewhat secure. Students (88%) reported that they surf the web at their university with behaviours that are different than what they employ at home. According to this survey, 18% of students prefer not to or are unable to access the Internet at university.

  This trend confirms that informal regulations of Internet cafes have changed users' access behaviours and created a sense of caution when they use their networks.

- **Perceptions of monitoring and confirmed censorship do not necessarily translate into users using tools to seek security or access information.**

While many felt that they are being subjected to surveillance, most respondents (71%) reported not using any means to protect their privacy online.

In the question, anonymity and identity protection tools were given as examples for means to protect identity. This was slightly different in the findings of the students' survey where almost 44% of responding students reported using specific tools and techniques to keep themselves anonymous and/or to protect their identity.

When it comes to using tools to regulate content and prevent access to undesired websites, most respondents (68%) reported their knowledge of desktop applications that allow them to customize access to undesired online content. However, knowledge does not mean application because 84% do not use this software. Students, again, have more interest in using tools to circumvent censorship —59% of students ordinarily use technical tools and software to gain access to blocked websites.

IX. Findings and Conclusion

- **The formal system of digital content governance is an extension of the general overlapping system of governance in Jordan, involving several executive entities with legislative powers.**

  The unclear boundaries between the legislative, judiciary, and executive governing entities in Jordan extend to the system governing the Internet's digital content. In Jordan, several public and private entities have overlapping executive and legislative jurisdictions on the production of and access to content. For example, the director of the Press and Publication Department has the authority to individually decide what constitutes a website and issue a blocking order based on his decision. The intelligence department, an executive entity, interferes with the legislation of policies including the Press and Publication Law that places restrictions on websites. Aside from legislating policy, the intelligence department interferes in the production of online content through requests to remove articles or through "friendly" threats to oppositional voices.

  Controls on information are also legislatively spread across the Internet Service Providers and telecom companies. ISPs have the authority to administratively suspend a service if it is proven to be violating what is called public morals or the public conduct. Certain ISPs have practised de facto blocking of some websites without any official or judiciary request. While the government's ISP, the National Information and Technology Center, executes blocking orders on the government network from different ministries, it still has authority over regulating the country-level domain name (ctLD): .JO. Being the registry and the registrar of .JO, NITC both places conditions and assesses applications for which websites names will be approved.

  The lack of a judicial process in regulating content removes citizens' rights to legally challenge the blocking order given it was based on the personal diligence of the Press and Publication director and the ISPs.

- **The lack of accountability systems paves the way for informal controls that prove to be a stronger mechanism for censorship and restrictions on speech.**

  While some information controls are practised through the rule of law, the most effective ones are informal. The weak system of accountability and the lack of judiciary review, in addition to the unregulated intimidation mechanisms from the intelligence department, intensify self-censorship. The lack of transparency in explaining and applying the laws and a lack of checks and balances allow the Ministry of Interior, General Intelligence Department, the NITC, and ISPs uncontested intervention in access and production of digital information. Surveys report that 85% of journalists avoid writing on topics critical of the regime, religions, or Gulf governors. Responses from surveys and focus groups have linked surveillance to digital self-censorship. These informal mechanisms of control have proven to be the most effective for information control, given that information never makes it to a publishing platform

- **The behind-the-scenes blocking techniques of ISPs pose an unexplored level of informal control that may further deprive users from their rights to access information.**

  The application of formal blocking requests reflects the underlying extent to which ISPs are participating in applying further controls beyond required blocking orders. The choice over which blocking technique to use could reflect both ISPs' blocking mentality and the available technologies and equipment in the ISPs' network that could stand between the user and the website that s/he attempts to access. Therefore, choosing to apply DNS tampering is choosing a way to relieve the ISP from legal liability. Paradoxically, it also leaves space for users to choose different features of the Internet that grant them access to any content. On the other hand, using a more complex technique, like TCP reset, reflects a sophisticated approach used by the ISP to gain full control over monitoring traffic and accessing data.

- **Legislations regulating online content lack technical understanding of the Internet's working,**

and therefore lead to confused labor-intensive applications of law.

In the legislation set to regulate content on this network there is a huge gap in the technical understanding of the Internet's nature as an interconnected network. Legislators' misunderstanding of the digital network's technicalities intensify the tension between Jordan's aspiration to open up its ICT market, and its desire to control online expression. An example of this misunderstanding is the tendency to extend the same restrictive legislations on print and publication to online media. Legislators say that they are only targeting electronic publications that work as local news websites. Attempting to draw local borders on digital content in an interconnected network has made it almost impossible to implement the law upon clear criteria because online content is not bound to a physical space. The poor understanding of digital content is also reflected in the legal references about electronic publication and what is considered news. Defining news as electronic publication ignores the decentralization of information production that the Internet provides.

Legislators' insistence that the term electronic publication doesn't include social media reflects their ignorance of how these platforms revolutionize news production and blur the lines between citizens and journalists.

The Information Crimes Systems law is another site of this gap in legal terminologies and technical realities of the Internet. The law criminalizes any illegal or unauthorized entry to a website—any website. This disregards the essential feature of websites being public in their nature without requiring an authorization for access.

The question of who controls online content is yet to be asked in a country that has been caught between maintaining its security and striving to become the Silicon Valley of the Middle East. It is an undeniable fact that the global environment has had an impact on the local economy of digital content. However, local controls have the most impact on restraining the free and open Internet environment that is necessary for development. Jordan witnessed the closure of several startups that developed social media platforms replicating YouTube (ikbis.com) and Twitter (watwet.com) as a result of their inability to compete with their international counterparts. Local controls contributes however to the stagnation in other digital content commercial entities or media platforms as 100 ICT companies have left the ICT market between 2012 and 2013. Many of these companies were online content companies affected by the introduction of Press and Publication law amendments

This report has introduced the formal and informal controls practiced on the access to and production of digital information in Jordan. It documents state attitudes toward the information flow that the Internet represents. First, it historically explains the security attitude toward the free flow of information in Jordan through court cases. Second, it maps the different jurisdictions across different public and private entities that hold executive power to translate the state's attitude into security practices. Third, it highlights the results of technical testing that peels back another layer of informal control practices by telecommunication companies. It also draws connections between formal and informal controls and people's experiences based on an online survey, focus groups, and interviews with lawyers and journalists. It separates the results of an online survey to highlight the implications of these formal and informal tools on the online users' experiences.

Although there are limitations in measuring the scale to which these controls affect the evolution of media in Jordan and its creative market economy, we hope this paper can serve as a base for further research on the extent to which this information control apparatus affects the evolution of digital content production across commercial entities: from the work of NGOs to active Jordanian groups and media platforms. It will be both interesting and important to explore changes in the users' behaviors to adapt or overcome such controls. We also hope that anecdotes and perceptions about online surveillance that were revealed in surveys and focus groups will mark the beginning of a serious effort to explore the state of surveillance in Jordan, and the impact of people's perceptions of surveillance on freedom of expression and content creation. We hope that this paper will initiate a move toward a more informed discussion and advocacy initiatives that attempt to change this restrictive reality of a network that is essential for social, economic, and political development in Jordan.

Appendix 1. Perceptions of Online Monitoring in Jordan [Survey in Arabic]

1. Age Group:
    - Below 20
    - 21–30
    - 31–40
    - 41–50
    - Above 50
2. Gender
3. Do you reside in Jordan? (*Yes, No*)
4. District
5. Using the answers *absolute secure, somewhat secure, not secure at all, does not apply*, to what extent do you feel secure when using the Internet from
    - Home
    - Work
    - Mobile
    - University
    - Internet café?
6. Do you believe that official entities are collecting and storing your personal information and interactions online? (*Yes, No, I don't know*)
7. Do you use any tools to protect your privacy online? (anonymity or identity- protection programs) (*Yes, No*)
8. Do you practise self-censorship on content you post or share online? (*Yes, No*)
9. Do you believe that the following types of monitoring exist online:
    - Official monitoring
    - Friends and family
    - Employer
    - Different user groups online?
10. In case you believe monitoring exists, to what extent (*to a large extent, to a small extent, does not affect*) are your online interactions (navigation or publishing) affected by monitoring of the following entities:
    - Government
    - Family members

- Employer
- Different user groups online

11. To what extent are you aware of the laws that regulate online content? (*very aware, slightly aware, not aware*)

    - Privacy policy and usage rights between you and your ISP
    - Press and Publication Law
    - Telecommunication Law
    - Information Systems Crimes Law

12. Do you think that online content needs regulation by an official entity? (*Yes, No*)

13. Are you aware of any programs or tools available for you to download on your personal computer that allow you to block undesired websites?

14. If your answer to the previous question was *yes*, do you use these tools in your home or work?

Appendix 2. Perceptions of Online Monitoring in Universities [Survey in Arabic]

1. Age
2. Gender
3. Do you reside in Jordan (*Yes, No*)
4. University
5. Do you access the Internet through the university network? (*Yes, No*)
6. On daily basis, how long do you access your university network:
    - Less than an hour
    - 2–3 hours
    - More than three hours
    - I don't access university network on daily basis
7. Do you need an account to log in to the network? (*Yes, No*)
8. Do you think your activities on the university network are being monitored? (*Yes, No*)
9. If yes, by whom?
10. What kind of online activities do you believe are being monitored?
    - browsing history
    - social media interactions
    - university email
    - I don't know
11. Do you use techniques to protect your privacy online while using the university network? (*Yes, No*)
12. Describe the tools/techniques you use:
13. Do you think there are blocked websites on your university network?
14. Describe blocked websites, and mention URLs if available.
15. Describe what made you believe that you are being monitored?
16. Does your university have an Internet usage policy? (*Yes, No, I don't know*)

Appendix 3. Network Measurement Results

In August and September of 2013, the 7iber research team in collaboration with the Cyber Stewards program at the University of Toronto conducted network measurement tests in Jordan on four ISPs to identify national-level Internet censorship.

The tests used a custom-designed network-measurement tool. This software tool, written in Python, runs from a computer located in the country of interest, in this case Jordan. The tool attempts to simultaneously access a list of websites from both Jordan and from a control location at the University of Toronto which does not censor the types of content being tested for. By comparing the results of these simultaneous attempts to access websites, we can determine whether any websites are being deliberately censored. To account for intermittent network issues that may prevent access to a site but that do not represent deliberate censorship, we conduct multiple tests over multiple days.

A number of data points are gathered for each attempt to access a URL: HTTP headers and status code, IP addresses, page body, trace routes, and packet captures. Through a process of both automated and manual analysis, we determine differences in the results returned from Jordan and the control location to identify instances of deliberate filtering. Because there are often legitimate reasons that content will differ in Jordan and at the University of Toronto (such as a domain resolving to a different IP address for load balancing, or content displaying in different languages) manual inspection of the results is necessary. If and when we identify an instance of deliberate filtering, our analysis system is configured to identify the signature of a deliberately blocked site (like, for example, always resolving to the same incorrect IP address) to speed up future analysis.

This testing was conducted on the ISPs Orange, Mada, Zain, and Umniah. A total of 182 unique URLs were tested. All of the URLs tested were websites of Jordanian news organizations that had been reported as blocked or at risk of being blocked. Since this was a very focused testing sample, we cannot extrapolate from these results the proportion of sites blocked in general or what other types of content may be blocked.

Blocking was identified on all four ISPs tested, however the method and degree of blocking varied among all four. A total of 113 URLs were blocked on the Orange ISP as a result of DNS tampering. On the ISP Mada, ninety URLs were found to be blocked as a result of DNS tampering (87 URLs) and a failure to respond to the TCP handshake request (3 URLs). Testing on the Zain ISP found seventy-five URLs blocked as a result of TCP reset (“RST”) packet injection. Finally, thirty-five URLs were blocked on the Umniah ISP as a result of DNS tampering.

In the case of Orange, domain names were blocked through DNS tampering. DNS is the service used to translate (or “resolve”) a domain name (such as “7iber.com”) to an IP address (e.g., 192.168.0.1). A censor can implement censorship by returning an incorrect IP address for a particular domain name, or not returning an IP address at all. However, DNS tampering is often the easiest censorship method to circumvent because users can configure their computers to use an alternative DNS service or access websites directly by IP address. In the case of Orange, 113 URLs resolved to 169.254.5.190 and 169.254.254.169, which are non-routable IP addresses.

Similarly, attempts to access eighty-seven URLs on Mada simply failed to return an IP address at all during the DNS resolution process. Mada also implemented an additional method of filtering, which was blocking a response during the TCP handshake process. When a client attempts to access a website, the client and server initiate the connection through what is known as a TCP handshake. For the three URLs identified, there was no response to the initial TCP handshake request from the client, despite the website being accessible from the control location. This is potentially the result of the censored website’s IP address being blocked entirely, preventing any traffic from reaching the censored website server. It is not entirely clear why multiple methods of censorship would be used on the same ISP. The different methods would, however, require different methods of circumvention. In other words, the use of an alternative DNS service to circumvent DNS tampering would not be effective if all traffic between the client and censored server is blocked.

A third method of censorship was identified on the Zain ISP. Here, we identified seventy-five URLs that

were blocked as the result of the injection of TCP RST packets. In this method of censorship, a middlebox (a device located between the user and the censored webserver) injects a fraudulent packet signaling to both the client and server to sever the connection. This is a less common method of censorship since it is more technically intensive than most other methods.

Finally, thirty-five URLs were found blocked on the Umniah ISP as a result of a failure to return an IP address during the DNS resolution process. This is the same method that the Mada ISP was using.[65]

65

Details on the list of blocked websites and blocking techniques across all ISPs networks in June 2013, across different connections: ZainJo, Orange, Umniah
https://docs.google.com/spreadsheet/pub?key=0Ahnrw9TXcBQ3dE5CbHdFT0c3aHpyajJlSmFKRTNrUFE&output=html