access

IRAQ'S INFORMATION TECHNOLOGY CRIMES ACT OF 2011: VAGUE, OVERBROAD, AND OVERLY HARSH

April 2012

IRAQ'S INFORMATION TECHNOLOGY CRIMES ACT OF 2011: VAGUE, OVERBROAD, AND OVERLY HARSH

The political environment in Iraq has become increasingly closed under the government of Prime Minister Nouri al-Maliki. Following the official withdrawal of U.S. troops from Iraq, and with international attention focused on the ongoing fallout from the 2011 Arab uprisings, there has been a consolidation of judicial, security, and political power. This is evidenced by three new draft laws[1] and the recently passed Journalists Rights Law, which together limit the freedoms of speech, expression and association.[2]

In this already volatile context, lawmakers are planning to pass another law that further illegitimates speech and expression—this time online. At the end of last year, the Presidential Council approved the Iraqi Informatics Crimes Law,[3] published as the Information Technology Crimes (ITC) Act in an English language draft.[4] The ITC Act, which has had a first reading in Iraqi Parliament, will come to a vote in the Council of Representatives in April 2012.

The broadly worded ITC Act declares that it "aims at providing legal protection for the legal use of the computer hardware and the internet," and affects the public sector, the media, corporations, finance, and civil society. Its impact, however, is to narrowly define legal behaviors online and empower authorities to restrict unwelcome speech and criticism. Indeed, the law's Purpose clause refers to "great causalities" inflicted on "institutions and individuals," perpetrated by computer and internet users, that "threaten the national security and national sovereignty, weaken the confidence in the new technologies," and "threaten the human creativity."

These statements fly in the face of Iraqis' increasing preference for electronic media. A recent survey commissioned by IREX noted that 33% of Iraqis use their mobile phone to get news and information and 28% use the internet for news.[5] Facebook users and bloggers[6] have boomed exponentially in the last 12 months. Repression of demonstrations in the Kurdistan Region pushed people off the streets and online. Today, Facebook pages exist on almost every subject of interest to a robust civil society, including the proposed ITC Act.[7] Telecom operators are pushing for 3G networks. But with this Act on the books and no education about cyber laws available to them, thousands of young people could end up facing prison sentences or worse for their comments on Facebook forums. The dangers are real. Outspoken journalist Hadi al-Mahdi warned of threats on his Facebook page before his assassination on September 8, 2011.[8]

The ITC Act attempts to bolster privacy and security by restricting the ways private companies handle and share user information. It acknowledges corruption by increasing penalties for those who target the public sector and government data. But the law (still in draft form) has dangerous implications for respect of civil liberties, activists, civic actors, and the press. Furthermore, the criminal sanctions it proposes are wildly disproportionate in both scope and severity. Given its extremely broad and vague wording, the law systematically lacks clarity and legal certainty. We see a number of specific areas of concern:

1 Draft Commission of Media and Communication Law; the draft Political Parties Law; and the draft Law of Expression, Assembly, and Peaceful Protest.

2 *Freedoms in Iraq: An Increasingly Repressive Legal Net*, IREX, Centre for Law and Democracy <http://irex.org/sites/default/files/Report.Iraq-Freedoms.with-cover%20for%20web.pdf>

3 <http://www.law-democracy.org/wp-content/uploads/2012/01/Iraq.Informatics-Crime.Aug11.pdf>; <http://www.article19.org/resources.php/resource/2792/en/iraq:-draft-informatics-crimes-law>

4 Find a copy of the 2011 ITC Act here: <http://www.slideshare.net/hamzoz/informatics-crimes-in-iraq>

5 IREX, Iraq 2011 Media Usage Survey, <http://irex.org/resource/iraq-2011-media-usage-survey>

6 Iraq Blog Count, <http://iraqblogcountexp.blogspot.com>

7 <https://www.facebook.com/No4ICLinIraq>

8 Washington Post, Hadi al-Mahdi, slain Iraqi journalist, had warned of threats, <http://www.washingtonpost.com/world/middle-east/hadi-al-mahdi-slain-iraqi-journalist-had-warned-of-threats/2011/09/09/gIQAsy52DK_story.html>

- **Vagueness and overbreadth in definitions of crimes**
- **Harsh punishments without proportionality**
- **Lack of protection for the press, whistleblowers, and others**
- **Uncertainty and lack of privacy for website operators, ISPs, and citizen users**
- **Excessive copyright enforcement**

VAGUENESS AND OVERBREADTH IN DEFINITIONS OF CRIMES

Certainty is important in the criminal realm. When one cannot reasonably understand what behaviors are proscribed, a law is too vague; when a law criminalizes legal as well as illegal activity, it is overbroad.

Unlimited Scope and Chilling Effects

Article 3 decrees life imprisonment for using a computer and the internet to: "affect…the unity of the country" and its economic, political, or security interests; deal with "the enemy" in order to endanger the nation; or harm or threaten military and intelligence computer and information systems, including through copying with criminal intent. A strict reading of the first two provisions invokes the traditional notions of treason and attempting to overthrow the government, and the third clause invokes Wikileaks-type hackers. Broadly interpreted, though, this law could be applied to anyone who speaks out against the government—a carte blanche for political repression.

Article 3 allows for prosecutions based on crimes against the country's "unity," "politics" and "interests," all malleable terms in the hands of overzealous prosecutors. The following vague crimes are also punishable by life imprisonment:

- Setting up or managing a website to promote terrorist "ideas" (Art. 4, Second)
- Promoting or publishing information about using "mind altering substances and the like" (Art. 5, Second)
- Using the internet to "harm the reputation of the country" (Art. 6, First)
- Disseminating "shaded facts in order to weaken the confidence" in the economy or financial systems (Art. 6, Third)

Without a clear idea of what these clauses mean, civil society actors may self-censor to avoid possible liability, creating a "chilling effect" on free expression.

Threats and Incitement

Article 11 prohibits threatening others through the internet or electronic communications with the intent of intimidation, or causing action or inaction. It lacks the key components of "likelihood" and "imminence"—the concept of idle or impossible threats, for example, versus incitement of a crowd already assembled and ready to take violent action.

Similarly, the anti-terrorism provisions in Article 4 lack any nexus between thoughts or ideas and their actual likelihood to cause imminent violence. In light of Iraq's violent past and present, lawmakers may be motivated to sharply punish incitement to violence. However, more clarity is needed to distinguish incitement from important discourse on security matters.

The vagueness of the Act stands in sharp contrast to the harsh penalties it delivers, and could enable the government to put political opponents away for good.

HARSH PUNISHMENTS WITHOUT PROPORTIONALITY

Harsh Punishments

Articles 3, 4, and 5 of the Act mandate overly harsh sentences of life imprisonment and fines of up to 50 million dinars, or around $50,000 USD—many times the average Iraqi income of around $3,300—for a variety of computer-based crimes, from organizing treasonous, terrorist, and human trafficking activities to publishing websites promoting narcotic use.

No matter the offense, life imprisonment is a severe penalty. The International Criminal Court, which has jurisdiction over the major crimes of Genocide, Crimes Against Humanity, War Crimes, and Aggression, only allows life imprisonment—its strictest punishment—"when justified by the extreme gravity of the crime and the individual circumstances of the convicted person."[9]

However, Articles 3 through 5 of Iraq's proposed ITC Act are far from limited to addressing crimes against humanity. They deal with a number of topics, including the aforementioned national security and anti-terrorism language, prohibitions on damaging or copying military or intelligence systems, and bans on promotion or facilitation of human trafficking or drug use. The Articles do not weigh the gravity of the crimes, but instead levy blanket and mandatory sentences of life imprisonment and a fine of 25-50 million Iraqi dinars (roughly $25-50,000 USD), not tailored to the particular circumstances of the offender or the offense.

No Proportionality

Not only are the punishments harsh, but these Articles also lack guidelines of scale or proportionality—the idea that the punishment fit the crime.[10] For example, Article 5 haphazardly punishes human trafficking websites alongside those promoting drug use. Its first clause forbids anyone to "set up a website or publish information" to conduct human trafficking, or to facilitate or promote "any form" of it, with a sentence of life imprisonment and a fine of 30-40 million Iraqi dinars (roughly $30-40,000 USD). The second clause prohibits publishing websites or information on "narcotic or mind altering substances and the like." It's possible that under Article 5, someone publishing a single blog entry on unapproved generic drugs could spend the rest of their life in jail. Worse still, this provision's broadly worded language could also be used to target online intermediaries like YouTube and Facebook if a single one of their users posts about human trafficking or drugs. Nothing in the Act clearly distinguishes internet service providers (ISPs), or intermediaries, from their end users, enabling prosecution of ISPs for the actions of millions of customers.

Destruction of Evidence

Article 29 allows judges to order the destruction of evidence, declaring, "the court may decide to confiscate or damage the tools, equipment, software, and devices used in the commission of the crimes stipulated in this Act." The Act does not state when in the conviction process such an order can be issued, which could easily open the door to the government seizing and destroying the property of their political opponents with little to no judicial intervention, due process, or proof of wrongdoing. Moreover, destruction of evidence will likely prejudice the appeals process, and even if convictions are overturned on appeal, justice may be unattainable if the files or hardware in question have already been deleted or destroyed. It should go without saying that in any democracy, information and evidence at issue should always be preserved until all judicial remedies are exhausted.

LACK OF PROTECTION FOR THE PRESS, WHISTLEBLOWERS, AND OTHERS

Freedom of Speech and the Press

Democratic politics require that the public enjoy freedom to criticize government officials and institutions. A robust news media cannot exist under the constant threat of defamation lawsuits and criminal libel prosecutions. Independent journalists, like those in Iraq's emergent citizen journalism culture, have even less support and capacity for legal battles than traditional media outlets. Article 22 (Third) punishes those who use the internet "to attribute terms, images, sounds or any other means that include libel and insult to the others." Will there be any flexibility in this law to poke fun at public figures? What about political cartoons? Indeed, it seems that any criticism of the government, corporations, or even private individuals might constitute "an insult," presenting a serious chilling effect on the exercise of free speech.

9 <http://untreaty.un.org/cod/icc/statute/99_corr/cstatute.htm> (Art. 77). Iraq, which is not a signatory to the Rome Statute of the International Criminal Court, announced in 2005 its intention to accede, then abruptly revoked its decision. See <http://www.rferl.org/content/article/1057782.html>.

10 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1431179>

Individuals and news outlets may be likely to self-censor to avoid the harsh sanctions of the libel clause, which mandates imprisonment of up to two years and a fine of 3-5 million dinars.

More serious threats to the media are in Article 6, which prohibits establishing or managing a website with the aim to "incite sectarian or sectarian trends, incite seditions, disturb security and public order, or harm the reputation of the country," punishable by life imprisonment. This overbroad Article seems ripe for abuse by a government seeking to silence its critics, and with the sentence of life in prison, this could effectively mean permanently silencing these voices.

Likewise, Article 4 prohibits promotion of terrorist acts or ideas, and Article 3 bans dealing with "the enemy" via computers or the internet. It's possible that a future government may label any nation that provides funding to civil society groups an "enemy," putting these activists at great risk. Indeed, these provisions make it unlikely there will be adequate space online for forums, news, and opinion writing addressing religious groups, political rights, and current events. Will journalists, academics and citizens be allowed to freely converse on these important topics, or interview opposition political figures? It seems unlikely.

Morality and the Public Interest

A "public interest" exception might improve the strong privacy protection in Article 21 (Third). The Article fines and imprisons for at least a year "whoever violates, in any manner, the religious, moral, family, or the social principles or values, or violates the privacy of the private life by using the information network or the computers in any manner." In many public interest news stories, including crime and health reporting, private family matters can become important topics of public discourse; under this broadly worded statute, this reporting could be censored. Without freedom to discuss private issues in public, few civic campaigns will get off the ground. Again, this statute, with its extremely broad and vague language criminalizing those who violate "principles" and "social values," could easily be used by the Iraqi government or its allies as cover to crack down on free speech, or even hide government misdeeds.

Article 19 (First, A) criminalizes publication of data gotten illegally, with intent to harm others. This provision could easily derogate the human rights to free speech and the press without an exception for information gotten and published in the public interest.

Financial Data, Corruption, and Whistleblowers

Articles 7 through 10 detail a range of penalties for disrupting and falsifying financial communications and documents, as well as manipulation and embezzlement of currencies, markets, and data. They target forgery and use of fake credit cards, tampering with stocks, deeds, and currency prices, and selling or operating the software, the websites and the hardware that make counterfeiting, money laundering, and financial fraud possible.

These Articles are reasonably written and clearly require intentional, knowing wrongdoing. The provisions increase penalties—"temporary detention" and fines ratchet up to mandatory ten-year prison sentences—for those misusing or targeting government and public sector funds, demonstrating intent to root out corruption. But to expose corruption, especially in the government and financial sectors, society often needs the help of people with access to private or protected financial records and documents. Articles 7 through 10 do not leave room for legitimate reasons to intercept or expose financial data, such as to reveal fraud.

Iraq needs specific protection for such "whistleblowers." Indeed, as currently written, the Act would prevent the press and reporters from being allowed to access and publish sensitive records for the purposes of revealing important news to the public. Currently, Article 9 provides for the imprisonment of "whoever abstracts or appropriates intentionally" another's email or financial record "to achieve a benefit to him or to others." Hypothetically, a journalist who received an anonymous delivery of a corrupt government official's bank statements or records of emails soliciting bribes could be prosecuted under this Act.

UNCERTAINTY AND LACK OF PRIVACY FOR WEBSITE OPERATORS, ISPS, AND CITIZEN USERS

Articles 14 through 22 are a hodgepodge of rules on computer and internet operators and users in the realms of intellectual property, privacy, and consumer rights, lacking a comprehensive scheme of crimes or penalties.

Data Storage, Transfer, and Handover to Authorities

Telecommunication and internet companies are broadly forced by Articles 13 and 18 to reveal their users' data. Civil liberties also suffer under Article 18, which criminalizes those who give false data to or "decline to provide information or data to the judicial or administrative authorities." Similarly, Article 13 sanctions "whoever declines to provide the security authorities and bodies responsible for issuing [electronic] licenses with the required reports, information and statistics…to the extent that relates to their activities" and does not violate intellectual property rights. These provisions fail to provide for any privacy safeguards, do not require authorities to produce warrants, and could force news media to reveal their sources, which further discourages whistleblowers.

The government officials making requests, including "administrative" and "security authorities" and "bodies responsible," go undefined. There is significant difference between judicial authorities and these far more nebulous (and often less rights-respecting) bodies, leading to a situation where unaccountable entities could demand user data. Indeed, the notion that "administrative" and "security authorities" can request information about users absent any judicial intervention or due process creates an environment where a police state can thrive.

Access supports sanctions in Article 19 (First, C) on those who "sell, transfer, or trade" subscribers' personal data without their permission. But Article 19 also declares that no one may disclose subscriber information, secrets or login data without prior approval by a "competent official body." What or whom constitutes a "competent official body"? Does that refer to a warrant requirement? How does it comport with Article 18's demand that operators hand over data to the authorities?

Rules Regarding Internet Use

Article 14 prescribes a maximum penalty of three months imprisonment and a 5 million Iraqi dinar fine for doing a number of things online, including: "intrude, bother, or call the users of the computers and the internet without permission" or "hinder" them. This clause could inhibit innovation by online businesses afraid to "bother" users, and, ironically, might "hinder" internet users more than the outlawed activities.

Article 18 attacks anonymity by outlawing the use of a "false identity or name" or an "unreal or illusory website" with the intent of "deception and fraud." Perhaps aiming at phishing sites, the Act does not define unreal, illusory, fraud, and deception. Without clarifications, the law's mandatory sentence, of up to three years imprisonment and 2 to 3 million dinar fines, risks seriously impinging on internet freedom. Anonymity and privacy have been the cornerstone of many legitimate uses of the internet, as well as a critical blanket of protection for online activists. It is not necessary to criminalize anonymity if the offender has been identified and the fraud already proven. Additionally, without requiring a criminal intent beyond simple deception, the law captures pure speech and expression, inhibiting social, cultural, and political rights.

Aimed at malicious hackers, Article 21 (First, B) forbids accessing "the website of a company, institution or others to change, delete, or modify the design of this website or exploit it unlawfully." The limits of "exploit" are undefined and widely open to interpretation. A better treatment of hacking and website defacement might address the threshold crime of unauthorized access, modification, or impairment of data and systems, then add penalties based on the severity of any crimes intended or committed thereafter.[11] Such a law would avoid language like "website" and better adapt to changing technology, methods of disruption, and harms.

11 See Australia's Cybercrime Act 2001, sec. 477.1 <http://www.comlaw.gov.au/Details/C2004A00937>

EXCESSIVE COPYRIGHT ENFORCEMENT

A broad attempt to respect intellectual property in Article 21 fines and imprisons for two to three years those who, "Use the internet and the computer to publish or copy intellectual works, literary works, or scientific research belonging to others and that protected by laws or international conventions." This provision does not contain any "fair use" exemptions that would allow for lawful, non-infringing copying or use of protected works, such as for the purposes of commentary, satire, remixing, or documentary filmmaking. Furthermore, protections should be made for educational and other non-economic uses. There are abundant examples of model legislation and recommendations that would be appropriate here.[12] Moreover, criminal sanctions (as opposed to civil damages) should not be imposed for activities like infringement that are essentially economic in nature.

The intellectual property clause in Article 21 (First) is followed by the clause aimed at malicious hackers. The Article fails to provide any rationale for putting an action like website defacement in the same category, deserving of the same punishment, as copying of a protected work, even for personal, non-infringing use.

CONCLUSION AND RECOMMENDATIONS

The Iraqi Information Technology Crimes Act is a very ambitious attempt to synthesize concerns for privacy, anti-corruption, digital copyright enforcement, and data security with national economic, political, and security interests. It establishes vague and overbroad crimes, creating a chilling effect on speech. Extremely harsh punishments are mixed among fines and misdemeanor penalties for rather benign crimes, with no attention to scale, necessity, or proportionality. The Act fails to protect ISPs and intermediaries, civil liberties, the press and whistleblowers. Information and data protection clauses lack uniformity and seemed designed for yesterday's crimes rather than emerging technology. Data handover mandates need privacy and warrant safeguards.

The Act affects a wide cross-section of Iraqi society, including journalists, commerce, the IT sector, and even political parties. The Iraqi government would do well to properly and publicly consult those whom this law will affect, including the Iraqi blogger community, already organizing against the Act.[13] Given the myriad problems with the Act and its easily abused provisions, it is critical that the Iraqi government conduct a proper human rights impact assessment of the Act and engage with national and international civil society actors to rewrite this draft law.

12 American Society of International Law <http://www.asil.org/erg/?page=iipl>

13 c.f., <https://www.facebook.com/No4ICLinIraq> and; <https://1stconference4iraqibloggers.wordpress.com>