

THE INTERNET IN THE MIDEAST
AND NORTH AFRICA

FREE EXPRESSION AND CENSORSHIP

HUMAN RIGHTS WATCH
NEW YORK · WASHINGTON · LONDON · BRUSSELS

COPYRIGHT © JUNE 1999 BY HUMAN RIGHTS WATCH
ALL RIGHTS RESERVED.
PRINTED IN THE UNITED STATES OF AMERICA

ISBN 1-56432-235-1
LIBRARY OF CONGRESS CATALOG CARD NUMBER 99-64033

ADDRESSES FOR HUMAN RIGHTS WATCH

350 FIFTH AVENUE, 34TH FLOOR, NEW YORK, NY 10118-3299
TEL: (212) 290-4700, FAX: (212) 736-1300, E-MAIL: HRWNYC@HRW.ORG

1630 CONNECTICUT AVENUE N.W. SUITE 500, WASHINGTON, DC 20009
TEL: (202) 612-4321, FAX: (202) 612-4333, E-MAIL: HRWDC@HRW.ORG

33 ISLINGTON HIGH STREET, N1 9LH LONDON, UK
TEL: (171) 713-1995, FAX: (171) 713-1800, E-MAIL: HRWATCHUK@GN.ORG

15 RUE VAN CAMPENHOUT, 1000 BRUSSELS, BELGIUM
TEL: (2) 723-2009, FAX: (2) 732-0471, E-MAIL: HRWATCHEU@SKYNET.BE

WEB SITE ADDRESS: [HTTP://WWW.HRW.ORG](http://www.hrw.org)

GOPHER ADDRESS: //GOPHER.HUMANRIGHTS.ORG:5000/11/INT/HUMAN RIGHTS WATCH

LISTSERV ADDRESS: TO SUBSCRIBE TO THE LIST, SEND AN E-MAIL MESSAGE TO MAJORDOMO@IGC.ORG WITH "SUBSCRIBE HUMAN RIGHTS WATCH-NEWS" IN THE BODY OF THE MESSAGE (LEAVE THE SUBJECT BLANK).

HUMAN RIGHTS WATCH

Human Rights Watch conducts regular, systematic investigations of human rights abuses in some seventy countries around the world. Our reputation for timely, reliable disclosures has made us an essential source of information for those concerned with human rights. We address the human rights practices of governments of all political stripes, of all geopolitical alignments, and of all ethnic and religious persuasions. Human Rights Watch defends freedom of thought and expression, due process and equal protection of the law, and a vigorous civil society; we document and denounce murders, disappearances, torture, arbitrary imprisonment, discrimination, and other abuses of internationally recognized human rights. Our goal is to hold governments accountable if they transgress the rights of their people.

Human Rights Watch began in 1978 with the founding of its Europe and Central Asia division (then known as Helsinki Watch). Today, it also includes divisions covering Africa, the Americas, Asia, and the Middle East. In addition, it includes three thematic divisions on arms, children's rights, and women's rights. It maintains offices in New York, Washington, Los Angeles, London, Brussels, Moscow, Dushanbe, Rio de Janeiro, and Hong Kong. Human Rights Watch is an independent, nongovernmental organization, supported by contributions from private individuals and foundations worldwide. It accepts no government funds, directly or indirectly.

The staff includes Kenneth Roth, executive director; Michele Alexander, development director; Reed Brody, advocacy director; Carroll Bogert, communications director; Cynthia Brown, program director; Barbara Guglielmo, finance and administration director; Jeri Laber special advisor; Lotte Leicht, Brussels office director; Patrick Minges, publications director; Susan Osnos, associate director; Jemera Rone, counsel; Wilder Tayler, general counsel; and Joanna Weschler, United Nations representative. Jonathan Fanton is the chair of the board. Robert L. Bernstein is the founding chair.

The regional directors of Human Rights Watch are Peter Takirambudde, Africa; José Miguel Vivanco, Americas; Sidney Jones, Asia; Holly Cartner, Europe and Central Asia; and Hanny Megally, Middle East and North Africa. The thematic division directors are Joost R. Hiltermann, arms; Lois Whitman, children's; and Regan Ralph, women's.

The members of the board of directors are Jonathan Fanton, chair; Lisa Anderson, Robert L. Bernstein, David M. Brown, William Carmichael, Dorothy Cullman, Gina Despres, Irene Diamond, Adrian W. DeWind, Fiona Druckenmiller, Edith Everett, Michael E. Gellert, Vartan Gregorian, Alice H. Henkin, James F. Hoge, Stephen L. Kass, Marina Pinto Kaufman, Bruce Klatsky, Joanne Leedom-Ackerman, Josh Mailman, Yolanda T. Moses, Samuel K. Murumba, Andrew Nathan, Jane Olson, Peter Osnos, Kathleen Peratis, Bruce Rabb, Sigrid Rausing, Orville Schell, Sid Sheinberg, Gary G. Sick, Malcolm Smith, Domna Stanton, and Maya Wiley. Robert L. Bernstein is the founding chair of Human Rights Watch.

Human Rights Watch is dedicated to protecting the human rights of people around the world.

We stand with victims and activists to prevent discrimination, to uphold political freedom, to protect people from inhumane conduct in wartime, and to bring offenders to justice.

We investigate and expose human rights violations and hold abusers accountable.

We challenge governments and those who hold power to end abusive practices and respect international human rights law.

We enlist the public and the international community to support the cause of human rights for all.

ABOUT THIS REPORT

THIS REPORT WAS RESEARCHED AND WRITTEN BY ERIC GOLDSTEIN, DEPUTY DIRECTOR OF THE MIDDLE EAST AND NORTH AFRICA DIVISION OF HUMAN RIGHTS WATCH. IT WAS EDITED BY HANNY MEGALLY, EXECUTIVE DIRECTOR OF THE DIVISION, DINAH POKEMPNER, DEPUTY GENERAL COUNSEL OF HUMAN RIGHTS WATCH, AND MICHAEL MCCLINTOCK, DEPUTY PROGRAM DIRECTOR. JAGDISH PARIKH, HUMAN RIGHTS WATCH'S ONLINE RESEARCH ASSOCIATE, PROVIDED HELPFUL COMMENTS ON THE DRAFT. WE ARE ALSO GRATEFUL FOR THE GENEROUS AND EXPERT INPUT OF OUTSIDE READERS GREY E. BURKHART AND DAVID BANISAR, WHO BEAR NO RESPONSIBILITY FOR ANY ASSERTIONS OR ERRORS IN THE REPORT. SARA EGGERLING, MIDDLE EAST AND NORTH AFRICA DIVISION ASSOCIATE, FORMATTED THE REPORT.

HUMAN RIGHTS WATCH WISHES TO THANK THE J.M. KAPLAN FUND FOR MAKING POSSIBLE THE TRANSLATION OF PORTIONS OF THIS REPORT INTO ARABIC.

NOTE: THIS REPORT CITES MANY WEB PAGES AND WEB-SITE ADDRESSES (UNIFORM RESOURCE LOCATORS, OR URLS). SINCE THE PREPARATION OF THE REPORT, SOME OF THESE MAY HAVE BEEN MODIFIED, RELOCATED, OR RENDERED UNAVAILABLE.

TABLE OF CONTENTS

I. SUMMARY	1
II. RECOMMENDATIONS	3
III. LEGAL STANDARDS PERTAINING TO ONLINE FREEDOM OF EXPRESSION.....	7
IV. INTRODUCTION	12
V. THE INTERNET IN THE MIDDLE EAST AND NORTH AFRICA: A CAUTIOUS START	16
VI. CYBERCENSORSHIP: ITS VARIOUS FORMS.....	27
VII. GOVERNMENT-IMPOSED FILTERING SCHEMES VIOLATE THE RIGHT TO FREE EXPRESSION.....	30
VIII. CONTENT AND CARRIER: THE QUESTION OF LIABILITY	34
IX. HOW USERS CAN PROTECT THEIR RIGHTS TO PRIVACY AND ANONYMITY	36
X. COUNTRY PROFILES	41
Bahrain	41
Iraq.....	42
Jordan.....	45
Morocco.....	49
Saudi Arabia.....	51
Syria.....	55
Tunisia	58
United Arab Emirates.....	66
APPENDIX A: TABLE SHOWING INTERNET USE IN THE MIDDLE EAST.....	71
APPENDIX B: UNIFORM LETTER REQUESTING INFORMATION ON INTERNET POLICIES, SENT BY HUMAN RIGHTS WATCH IN MAY 1999 TO GOVERNMENTS OF THE REGION.....	73
APPENDIX C: REPLIES TO HUMAN RIGHTS WATCH LETTER RECEIVED FROM OFFICIALS OF IRAQ, JORDAN, KUWAIT, QATAR, TUNISIA AND YEMEN.....	76

I. SUMMARY

THE INTERNET dramatically empowers persons in the exercise of their right to seek, receive, and impart information and ideas regardless of frontiers. Online communication must therefore be fully protected by international guarantees of the right to freedom of expression.

IN THE MIDDLE EAST AND NORTH AFRICA, Internet use is growing rapidly after a slow start. Today, all countries except Libya, Iraq, and Syria allow the public to access the Internet through a local service provider. But in a region where nearly all governments abridge the right to freedom of expression in significant ways, many have taken a cautious approach toward a medium that permits persons easily, inexpensively, and rapidly to exchange information in ways that elude state control.

GOVERNMENTS have adopted various means to restrict the flow of information online. Saudi Arabia, Yemen, and the United Arab Emirates impose censorship via proxy servers, devices that are interposed between the end-user and the Internet in order to filter and block specified content. In many countries, including Jordan, taxation and telecommunications policies keep Internet accounts quite costly and thus beyond the means of many—whether or not this is the objective of these policies. Tunisia has enacted the region's most detailed Internet-specific legislation, which is in large part designed to ensure that online speech does not escape the government's tough controls on critical speech in other media. In the majority of countries where Internet-specific laws have not been enacted, legal or de facto constraints on freedom of speech and of the press have a chilling effect on what is expressed online, especially in public forums like open bulletin boards and "chat-rooms" (online discussions where participants communicate in real time).

AND IN A REGION where many governments routinely tap the phones of dissidents, Internet users in many countries, including Bahrain and Tunisia, suspect that the right to privacy of correspondence is being violated by government surveillance of e-mail. One Bahraini spent more than a year in jail on suspicion of e-mailing "political" information to dissidents abroad.

FORTUNATELY, some governments in the region have taken a more hands-off attitude toward the Internet—even as they enforce laws that curb other means of expression. This has created paradoxical situations in Egypt and Jordan, where newspapers or articles that the authorities censored became quickly available online without repercussions for those who read, posted, or forwarded them. Algeria, Morocco, and the Palestinian Authority have made little if any effort so far to control online content, allowing Internet users access to a wealth of political and human rights information that the local print and broadcast media cannot publish.

THIS REPORT surveys in a noncomprehensive fashion the Internet policies of governments in the region as they affect the right to freedom of expression. Human Rights Watch identifies policies, laws, and practices that violate or endanger this right. By offering this critique while proposing a set of principles to guide policies and legislation, Human Rights Watch

SEEKS TO ENCOURAGE GOVERNMENTS TO STRENGTHEN PROTECTIONS FOR FREEDOM OF EXPRESSION AT THIS EARLY STAGE OF THE INTERNET'S DEVELOPMENT.

II. RECOMMENDATIONS

PROTECTING ONLINE FREEDOM OF EXPRESSION REQUIRES NOT ONLY INTERNET-SPECIFIC POLICIES THAT ARE RESPECTFUL OF RIGHTS BUT ALSO AN ENVIRONMENT IN WHICH FREE EXPRESSION MORE GENERALLY IS GUARANTEED. IN MANY COUNTRIES, ONLINE EXPRESSION IS INHIBITED LESS BY INTERNET-SPECIFIC REGULATIONS THAN BY PRE-EXISTING PRESS CODES, DEFAMATION LAWS, AND UNOFFICIAL "RED LINES."

THE RIGHT TO FREEDOM OF EXPRESSION INCLUDES THE RIGHT TO ACCESS ONLINE COMMUNICATION; THE RIGHT TO SEEK, RECEIVE, AND IMPART INFORMATION ONLINE WITHOUT ARBITRARY RESTRICTIONS; AND THE RIGHT TO COMMUNICATE PRIVATELY OR ANONYMOUSLY ONLINE.

TO PROTECT AND FOSTER THESE RIGHTS, GOVERNMENTS SHOULD ADHERE TO THE FOLLOWING PRINCIPLES IN THEIR POLICIES TOWARD THE INTERNET:

(1) ENSURE THE INTERNATIONAL RIGHT TO FREEDOM OF EXPRESSION GENERALLY, AND ENSURE THAT ALL REGULATIONS PERTAINING TO ELECTRONIC COMMUNICATIONS COMPORT WITH THAT RIGHT.

ALL LEGISLATION, POLICIES, AND PRACTICES, INCLUDING THOSE THAT PERTAIN TO THE INTERNET, SHOULD BE CONSISTENT WITH THE UNIVERSALLY RECOGNIZED RIGHT TO FREE EXPRESSION. THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS, WHICH HAS BEEN RATIFIED BY ALL BUT FIVE COUNTRIES IN THE REGION, GUARANTEES TO EVERY PERSON "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."

MANY COUNTRIES OF THE REGION HAVE PRESS LAWS AND PENAL CODES THAT INVITE ABUSE OF THE RIGHT TO FREE EXPRESSION IN VARIOUS WAYS. INTERNET REGULATIONS IN TUNISIA EXPLICITLY EXTEND CRIMINAL PENALTIES FOR DEFAMATION AND FALSE INFORMATION TO ONLINE SPEECH; INTERNET USERS IN QATAR ARE SUBJECTED TO A VAGUELY WORDED REQUIREMENT IN THEIR SERVICE CONTRACT THAT THEY REFRAIN FROM "CARRY[ING] OUT ANY ACTIVITY WHICH IS CONTRARY TO PUBLIC ORDER." JORDAN AND MOROCCO, MEANWHILE, HAVE NO INTERNET-SPECIFIC LAWS RESTRICTING FREE EXPRESSION; HOWEVER, BOTH HAVE LAWS THAT CURB PRESS FREEDOM, AND THOSE LAWS, SUCH AS THE ONES THAT PROHIBIT DEFAMING OR DISPARAGING THE MONARCHY, NARROW THE BOUNDARIES OF WHAT CAN BE EXPRESSED ONLINE.

(2) ACCESS TO THE INTERNET TO RECEIVE AND IMPART INFORMATION IS INTEGRAL TO THE RIGHT OF FREE EXPRESSION.

GOVERNMENTS SHOULD TAKE APPROPRIATE MEASURES TO FACILITATE AFFORDABLE ACCESS TO ALL WITHOUT DISCRIMINATION TO ONLINE MEANS OF COMMUNICATION. FOR EXAMPLE, SYRIA, WHERE SELECTED STATE INSTITUTIONS ARE CONNECTED TO THE INTERNET, SHOULD MOVE RAPIDLY TOWARD MAKING ACCESS AVAILABLE TO ORDINARY CITIZENS.

(3) CENSORING MECHANISMS, IF USED, SHOULD BE IN THE HANDS OF INDIVIDUAL USERS, NOT GOVERNMENTS.

END-USERS SHOULD HAVE THE SOLE RESPONSIBILITY IN DECIDING IF AND HOW TO FILTER OR BLOCK ONLINE CONTENT FOR THEMSELVES AND THEIR NON-ADULT CHARGES. GOVERNMENTS SHOULD ABOLISH OR AVOID REGULATIONS THAT EMPOWER OFFICIAL AGENCIES TO BLOCK ONLINE CONTENT.

USERS, IF THEY WISH, CAN CHOOSE FROM A WIDE RANGE OF FREE OR INEXPENSIVE SOFTWARE ("CENSORWARE") THAT FILTERS CONTENT ACCESSED FROM THE WORLD WIDE WEB. THEY CAN ALSO PURCHASE MODEM LOCKS AND OTHER DEVICES TO PREVENT UNSUPERVISED ACCESS BY THEIR CHILDREN.

THE GOVERNMENTS OF TUNISIA, SAUDI ARABIA, IRAN, AND THE UNITED ARAB EMIRATES ARE AMONG THOSE THAT BLOCK SELECTED WEB SITES DEALING WITH POLITICS OR HUMAN RIGHTS, THUS PREVENTING USERS IN THEIR RESPECTIVE COUNTRIES FROM ACCESSING THEM. THIS FORM OF CENSORSHIP VIOLATES THE RIGHTS OF PEOPLE TO RECEIVE AND IMPART INFORMATION AND SHOULD BE HALTED IMMEDIATELY.

(4) COMMON DATA CARRIERS, SUCH AS INTERNET SERVICE PROVIDERS, GENERALLY SHOULD NOT BE LIABLE FOR INTERNET CONTENT.

LAWS ASSIGNING LIABILITY FOR ONLINE CONTENT SHOULD TARGET THE CONTENT ORIGINATOR (FOR EXAMPLE, THE AUTHOR) AND NOT THE CARRIER OR CONDUIT (SUCH AS THE INTERNET SERVICE PROVIDER OR OWNER OF A COMPUTER THROUGH WHICH CONTENT WAS TRANSMITTED). LAWS TARGETING ISPS IMPOSE A HEAVY AND PERHAPS TECHNICALLY IMPOSSIBLE BURDEN ON THE DATA CARRIER, ONE THAT IS INCOMPATIBLE WITH PROTECTING THE RIGHT TO FREEDOM OF EXPRESSION ONLINE.

TUNISIA REQUIRES ISPS TO DESIGNATE A DIRECTOR WHO "ASSUMES RESPONSIBILITY, IN ACCORDANCE WITH THE...PRESS CODE, FOR THE CONTENT OF PAGES AND WEB PAGES AND SITES THAT THE ISP IS REQUESTED TO HOST ON ITS SERVERS." THE DECREE STATES THAT ISPS MUST ALLOW NOTHING TO "REMAIN" ON THEIR SERVERS THAT HARMS "PUBLIC ORDER AND GOOD MORALS." THIS TYPE OF LEGISLATION RUNS COUNTER TO THE PRINCIPLE OF FREE EXPRESSION ONLINE BY IMPOSING A REGULATORY BURDEN ON ISPS THAT—TO THE EXTENT THAT IT IS EVEN FEASIBLE GIVEN THE NATURE OF DATA FLOW ONLINE—FORCES THEM INTO THE ROLE OF CENSORS ON BEHALF OF THE STATE.

(5) STRONG ENCRYPTION SHOULD BE AVAILABLE TO INDIVIDUALS.

INDIVIDUALS SHOULD BE ABLE TO SEND AND RECEIVE ENCODED OR ENCRYPTED COMMUNICATIONS. THEY SHOULD NOT BE COMPELLED TO OBTAIN AUTHORIZATION TO DO SO; NOR SHOULD THEY BE COMPELLED TO PROVIDE IN ADVANCE TO THIRD PARTIES ACCESS TO ENCODING "KEYS" OR OTHER MECHANISMS THAT WOULD PERMIT THE DECODING OF THEIR COMMUNICATIONS. COUNTRIES THAT CURRENTLY BAR UNAUTHORIZED ENCRYPTION INCLUDE ISRAEL, SAUDI ARABIA, AND TUNISIA.

(6) GOVERNMENT SURVEILLANCE OF ELECTRONIC COMMUNICATIONS SHOULD NOT INFRINGE UNDULY ON THE RIGHT TO PRIVACY AND OTHER CIVIL RIGHTS, AND SHOULD BE SUBJECT TO THE REQUIREMENTS OF DUE PROCESS AND JUDICIAL SUPERVISION.

ONE ARGUMENT AGAINST CONTROLS ON ENCRYPTION IS THAT GOVERNMENTS RETAIN OTHER EFFECTIVE LAW ENFORCEMENT TOOLS, SUCH AS SURVEILLANCE, SEARCH, AND SEIZURE. HOWEVER, THESE SHOULD ALWAYS BE USED IN CONFORMITY WITH INTERNATIONAL HUMAN RIGHTS LAW AND THE REQUIREMENTS OF DUE PROCESS. IN PARTICULAR,

- INVESTIGATIONS OR SURVEILLANCE IN PUBLIC ONLINE FORUMS SHOULD ADHERE TO INTERNATIONAL STANDARDS PROTECTING THE RIGHTS TO FREEDOM OF ASSOCIATION AND POLITICAL ACTIVITY. SUCH GUIDELINES SHOULD BE MADE PUBLIC.
- GOVERNMENTS SHOULD NOT MONITOR INDIVIDUAL INTERNET USERS FOR CIVIL OR CRIMINAL INVESTIGATORY PURPOSES OR COLLECT INFORMATION ON THE WAY THEY USE THE INTERNET, EXCEPT PURSUANT TO A JUDICIAL PROCESS AND JUDICIAL OVERSIGHT THAT IS CONSISTENT WITH INTERNATIONALLY RECOGNIZED PRINCIPLES OF PRIVACY.
- GOVERNMENTAL SEARCHES OR SEIZURE OF ELECTRONIC COMMUNICATIONS SHOULD BE CONDUCTED PURSUANT TO LEGALLY AUTHORIZED PROCEDURES THAT REQUIRE THERE TO BE SUFFICIENT EVIDENCE THAT THE USER IS ENGAGED IN ILLEGAL ACTIVITY TO JUSTIFY THE SEARCH. ANY SUCH SEARCH SHOULD BE CONDUCTED UNDER JUDICIAL SUPERVISION.
- ANY SEARCH SHOULD BE NARROW IN ITS SCOPE AND EFFECT.¹

(7) INDIVIDUALS SHOULD HAVE THE RIGHT TO COMMUNICATE AND RECEIVE INFORMATION ANONYMOUSLY.

REGULATIONS SHOULD NOT UNREASONABLY REQUIRE IDENTIFICATION OF PERSONS WHEN THEY ACCESS THE INTERNET OR EXCHANGE INFORMATION AND OPINIONS ONLINE. ISPs SHOULD, WHEREVER PRACTICABLE, PRESERVE THE RIGHT OF USERS TO ACCESS THE INTERNET ANONYMOUSLY.

¹ THESE RECOMMENDATIONS ARE ADAPTED FROM THE OPEN INTERNET POLICY PRINCIPLES, WHICH WERE ADOPTED BY A PANEL OF EXPERTS IN 1997 AS A BLUEPRINT FOR POLICY-MAKERS, <[WWW.SOROS.ORG/PRINCIPLES.HTML](http://www.soros.org/principles.html)> AND <[WWW.SOROS.ORG/NEWS.HTML](http://www.soros.org/news.html)>.

Legislation in Tunisia requires Internet service providers to submit the names of their clients to the government on a monthly basis. Such a disclosure requirement constitutes by its sweeping nature a violation of the right to seek, receive, and impart ideas anonymously.

III. LEGAL STANDARDS PERTAINING TO ONLINE FREEDOM OF EXPRESSION

THE INTERNET REPRESENTS A MAJOR DEVELOPMENT IN ENABLING PERSONS TO COMMUNICATE WITH OTHERS AND TO OBTAIN INFORMATION. SOME HAVE COMPARED ITS IMPORTANCE TO THE INVENTION OF THE PRINTING PRESS.

IN THE VIEW OF HUMAN RIGHTS WATCH, THE RIGHTS TO FREEDOM OF EXPRESSION, INFORMATION, PRIVACY, AND FREE ASSOCIATION UNDER INTERNATIONAL LAW APPLY AS MUCH TO ONLINE COMMUNICATION AS TO OTHER FORMS OF INDIVIDUAL COMMUNICATION. WHILE INTERNATIONAL TREATIES AND INSTRUMENTS DO NOT ADDRESS ELECTRONIC SPEECH SPECIFICALLY, THEIR ASSERTION OF THE RIGHT TO "SEEK, RECEIVE AND IMPART INFORMATION AND IDEAS THROUGH ANY MEDIA AND REGARDLESS OF FRONTIERS" (EMPHASIS ADDED) IS CLEARLY APPLICABLE TO EXPRESSION VIA THE INTERNET.

ARTICLE 19 OF THE UNIVERSAL DECLARATION OF HUMAN RIGHTS PROCLAIMS:

EVERYONE HAS THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION; THIS RIGHT INCLUDES FREEDOM TO HOLD OPINIONS WITHOUT INTERFERENCE AND TO SEEK, RECEIVE AND IMPART INFORMATION AND IDEAS THROUGH ANY MEDIA AND REGARDLESS OF FRONTIERS.

ARTICLE 19 OF THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS (ICCPR) REAFFIRMS THAT EVERYONE'S RIGHT TO FREEDOM OF EXPRESSION "SHALL INCLUDE THE 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." ARTICLE 19 STATES, FURTHERMORE, THAT RESTRICTIONS ON THIS RIGHT "SHALL ONLY BE SUCH AS ARE PROVIDED BY LAW AND ARE NECESSARY: (A) FOR RESPECT OF THE RIGHTS OR REPUTATIONS OF OTHERS; (B) FOR THE PROTECTION OF NATIONAL SECURITY OR OF PUBLIC ORDER (*ORDRE PUBLIC*), OR OF PUBLIC HEALTH OR MORALS."² THE ICCPR HAS BEEN RATIFIED BY ALGERIA, EGYPT, IRAN, IRAQ, ISRAEL, JORDAN, LEBANON, KUWAIT, LIBYA, MOROCCO,

² THE JOHANNESBURG PRINCIPLES ON NATIONAL SECURITY, FREEDOM OF EXPRESSION AND ACCESS TO INFORMATION, PUT FORWARD ON OCTOBER 1, 1995 BY A GROUP OF EXPERTS IN INTERNATIONAL LAW, NATIONAL SECURITY, AND HUMAN RIGHTS, STATE THAT RESTRICTIONS ON FREEDOM OF EXPRESSION SHOULD BE PERMITTED ONLY WHEN "THE GOVERNMENT CAN DEMONSTRATE THAT THE RESTRICTION IS PRESCRIBED BY LAW AND IS NECESSARY IN A DEMOCRATIC SOCIETY TO PROTECT A LEGITIMATE NATIONAL SECURITY INTEREST" (PRINCIPLE 1.1, SECTION D). ACCORDING TO THE PRINCIPLES, THE BURDEN OF DEMONSTRATING THE VALIDITY OF THE RESTRICTION RESTS WITH THE GOVERNMENT. CRITICISM OF THE GOVERNMENT OR ITS LEADERS IS PROTECTED. IN ADDITION, A GOVERNMENT MUST DEMONSTRATE THAT "THE RESTRICTION IMPOSED IS THE LEAST RESTRICTIVE MEANS POSSIBLE FOR PROTECTING THAT INTEREST" (PRINCIPLE 1.3, SECTION B). COPIES OF THE JOHANNESBURG PRINCIPLES ARE AVAILABLE FROM ARTICLE 19 IN LONDON AND AT <www.osti.hu/colpi/819>.

Syria, Tunisia, and Yemen. It has not been ratified by Bahrain, Oman, Qatar, Saudi Arabia, and the United Arab Emirates.³

The Open Internet Policy Principles, declared in March 1997 by a working group of European and North American experts, point out:

The Internet does not exist in a legal vacuum. For the most part, existing laws can and should regulate conduct on the Internet to the same degree as other forms of conduct. Such laws may differ from country to country, but should conform with the applicable binding human rights obligations contained in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the European Convention on Human Rights.

Under international law, governments are allowed to restrict the free flow of information to protect certain narrow interests such as national security or public morals. But any prior censorship of material before it is published should be subjected to the strictest level of scrutiny in line with international standards, which normally includes inquiry into the interest sought to be protected, the seriousness of the threat, and whether there are alternate means of protecting that interest that are less restrictive of the right to free expression. Indeed, the American Convention on Human Rights states in Article 13 that the right to freedom of expression "shall not be subject to prior censorship." Filtering or blocking access to Internet material by a government amounts to pre-publication censorship. Virtually all governments in the Middle East that block content on the Internet suppress some material that is unquestionably legal. Moreover, none of the governments in the region make public how censorship is actually practiced and what sites are blocked, insulating their actions from any scrutiny or evaluation under international human rights standards. The decision of what to block, and what technology to use to block it, should be in the hands of end users, rather than governments. A variety of software programs is readily available to users for this purpose.

The Right to Privacy

³ For a list of countries that have ratified the ICCPR, see <www.un.org/depts/treaty/>.

THE FREEDOM FROM ARBITRARY AND UNLAWFUL INTERFERENCE WITH ONE'S PRIVACY AND CORRESPONDENCE IS PROTECTED IN INTERNATIONAL LAW, AND APPLIES TO ELECTRONIC COMMUNICATIONS.⁴ A CAPRICIOUS, UNJUST OR DISPROPORTIONATE INTERFERENCE WOULD BE "ARBITRARY," AS WOULD ONE THAT WAS FOR A PURPOSE INIMICAL TO THE PROTECTION OF HUMAN RIGHTS MORE GENERALLY, SUCH AS INHIBITING PEACEFUL DISSENT. STATES MAY NOT RANDOMLY OR FREELY INTERCEPT OR MONITOR E-MAIL OR INTERNET USAGE; IN THE NARROW CIRCUMSTANCES WHERE SURVEILLANCE CAN BE JUSTIFIED, IT MUST BE SUBJECT TO LIMITATION AND CONTROL TO AVOID INFRINGING THESE RIGHTS. MOREOVER, THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS REQUIRES STATES TO ACT POSITIVELY TO PROTECT INDIVIDUALS FROM SUCH INTERFERENCE WITH PRIVACY OR CORRESPONDENCE ON THE PART OF THIRD PARTIES SUCH AS NON-STATE ACTORS.⁵ ENCRYPTION, AS A TECHNOLOGY THAT PROTECTS COMMUNICATIONS AND CORRESPONDENCE FROM ARBITRARY INTERFERENCE, SHOULD BE LAWFUL AND ACCESSIBLE TO INDIVIDUAL USERS.

THE RIGHT TO COMMUNICATE ANONYMOUSLY

FREE EXPRESSION ENCOMPASSES A RIGHT TO COMMUNICATE ANONYMOUSLY. ANONYMITY IN COMMUNICATIONS IS CRITICAL TO THE RIGHT TO EXPRESS POLITICAL BELIEFS, AND TO SEEK AND IMPART INFORMATION WITHOUT FEAR OF RETRIBUTION. ANONYMITY HAS SERVED PERSONS WHO WISH TO PROVIDE ANONYMOUS TIPS TO JOURNALISTS OR "BLOW THE WHISTLE" ON IMPROPRIETIES IN THEIR WORKPLACE, AUTHORS WHO WISH TO WRITE UNDER ASSUMED NAMES, AND PARTICIPANTS IN SENSITIVE DISCUSSIONS, SUCH

⁴ THE UNIVERSAL DECLARATION OF HUMAN RIGHTS AFFIRMS IN ARTICLE 12, "NO ONE SHALL BE SUBJECTED TO ARBITRARY INTERFERENCE WITH HIS PRIVACY, FAMILY, HOME OR CORRESPONDENCE." THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS STATES IN ARTICLE 17, "NO ONE SHALL BE SUBJECTED TO ARBITRARY OR UNLAWFUL INTERFERENCE WITH HIS PRIVACY, FAMILY, HOME OR CORRESPONDENCE..." THE LANGUAGE OF THIS PROVISION IS BROAD ENOUGH TO ENCOMPASS ONLINE COMMUNICATIONS, INCLUDING ELECTRONIC MAIL AND NEWSGROUP POSTINGS.

⁵ THE ICCPR, ARTICLE 17(2), STATES, "EVERYONE HAS THE RIGHT TO THE PROTECTION OF THE LAW AGAINST SUCH INTERFERENCE OR ATTACKS." SEE ALSO MANFRED NOWAK, *UN. COVENANT ON CIVIL AND POLITICAL RIGHTS: CCPR COMMENTARY* (KEHL: N.P. ENGEL, 1993), PP. 289-290.

as an AIDS support group. The role of anonymous speech in fostering freedom of expression was eloquently defended thus:

DESPITE READERS' CURIOSITY AND THE PUBLIC'S INTEREST IN IDENTIFYING THE CREATOR OF A WORK OF ART, AN AUTHOR GENERALLY IS FREE TO DECIDE WHETHER OR NOT TO DISCLOSE HER TRUE IDENTITY. THE DECISION IN FAVOR OF ANONYMITY MAY BE MOTIVATED BY FEAR OF ECONOMIC OR OFFICIAL RETALIATION, BY CONCERN ABOUT SOCIAL OSTRACISM, OR MERELY BY A DESIRE TO PRESERVE AS MUCH OF ONE'S PRIVACY AS POSSIBLE. WHATEVER THE MOTIVATION MAY BE, AT LEAST IN THE FIELD OF LITERARY ENDEAVOR, THE INTEREST IN HAVING ANONYMOUS WORKS ENTER THE MARKETPLACE OF IDEAS UNQUESTIONABLY OUTWEIGHS ANY PUBLIC INTEREST IN REQUIRING DISCLOSURE AS A CONDITION OF ENTRY.⁶

ENCRYPTION

ENCODING ELECTRONIC COMMUNICATIONS ("ENCRYPTION"⁷) IS GROWING MORE COMMONPLACE, AND INDEED, IS COMMONLY RECOGNIZED AS ESSENTIAL TO FACILITATING THE GROWTH OF ELECTRONIC COMMERCE. "STRONG" ENCRYPTION SOFTWARE, THAT IS, CODING THAT IS NEARLY IMPOSSIBLE FOR THIRD PARTIES TO DECIPHER, IS WIDELY AVAILABLE NOW TO INDIVIDUALS AND BUSINESSES, WHERE ONCE IT WAS SOLELY USED BY GOVERNMENTS. ENCRYPTION PROTECTS PRIVACY OF COMMUNICATIONS, BUT EVEN MORE IMPORTANTLY, IT ENABLES THE FREE EXPRESSION OF IDEAS AND INFORMATION, PARTICULARLY WHERE THERE HAS BEEN A RECORD OF GOVERNMENT SURVEILLANCE AND REPRESSION. BY GUARANTEEING PRIVACY OF COMMUNICATIONS AND AUTHENTICATING THE IDENTITY OF COMMUNICATORS, ENCRYPTION ALSO ENABLES FREE ASSOCIATION BETWEEN INDIVIDUALS IN CYBERSPACE, AN IMPORTANT EXTENSION OF A TRADITIONAL RIGHT IN THE NEW CIRCUMSTANCES OF GLOBALIZATION.

⁶ EXCERPTED FROM THE DECISION OF THE U.S. SUPREME COURT IN *MACINTYRE V. OHIO ELECTIONS COMMISSION*, 514 U.S. 334 (1995).

⁷ ENCRYPTION INVOLVES ENCODING A TEXT PRIOR TO TRANSMISSION, THROUGH THE USE OF MATHEMATICAL LOGARITHMS, SO THAT IT CAN BE READ ONLY BY THE SENDER AND THE INTENDED RECIPIENT, WHO ARE IN POSSESSION OF "KEYS" THAT DECRYPT THE ENCODED TEXT AND PRESENT IT IN ITS ORIGINAL FORM.

WHILE THERE ARE LEGITIMATE LAW ENFORCEMENT CONCERNS THAT MUST BE TAKEN INTO ACCOUNT IN ANY NATIONAL POLICY ON ENCRYPTION, THERE IS NO JUSTIFICATION FOR EITHER BANNING INDIVIDUAL USE OF ENCRYPTION OR LICENSING USERS. ENCRYPTION SHOULD BE VIEWED AS A VEHICLE OF EXPRESSION LIKE A LANGUAGE; THE USE OF ENCRYPTION ALONE SHOULD NOT SUBJECT AN INDIVIDUAL TO CRIMINAL SANCTION, ANY MORE THAN SHOULD THE USE OF ESPERANTO OR SWAHILI TO COMMUNICATE.⁹ INDIVIDUALS SHOULD NOT BE REQUIRED TO OBTAIN AUTHORIZATION FROM THE AUTHORITIES IN ORDER TO SEND OR RECEIVE ENCRYPTED COMMUNICATIONS, NOR SHOULD THEY BE COMPELLED TO PROVIDE IN ADVANCE TO LAW ENFORCEMENT AUTHORITIES ACCESS TO KEY RECOVERY OR OTHER MECHANISMS THAT WOULD PERMIT THE DECODING OF THEIR COMMUNICATIONS. THESE ARE ALL OVER-BROAD POLICIES THAT PENALIZE LAW-ABIDING PERSONS.

ASSIGNING LIABILITY FOR ONLINE CONTENT

THE RIGHT TO FREE EXPRESSION IS BEST SERVED BY LAWS THAT FOCUS LIABILITY FOR SPEECH ON THE ORIGINATOR OF THE OFFENDING CONTENT, RATHER THAN ON ITS CONDUIT. ISPS DO NOT FIT NEATLY INTO ANY EXISTING MEDIA PARADIGM AND SHOULD NOT BE SUBJECTED TO REGULATORY STRUCTURES THAT MAY BE SUITABLE FOR OTHER TECHNOLOGIES OR MEDIA, SUCH AS A NEWSPAPER THAT CAN BE HELD LIABLE FOR ARTICLES APPEARING IN ITS PAGES. ISPS ACT MOST OF THE TIME MERELY AS CONDUITS OF INFORMATION (DATA CARRIERS, AKIN TO TELEPHONE COMPANIES), OFFERING THE TECHNICAL MEANS FOR USERS TO RECEIVE AND DISSEMINATE INFORMATION. IN MOST CASES, ISPS HAVE NO KNOWLEDGE OF THE CONTENT OF THE MESSAGES THEY TRANSMIT, OR EVEN OF THE WEB SITES THEY HOST—MANY OF WHICH ARE REVISED DAILY BY THEIR AUTHORS. THE SITUATION IS ARGUABLY DIFFERENT WHEN THE OFFENDING CONTENT IS CONTAINED IN MATERIAL OVER WHICH THE ISP EXERCISES EDITORIAL CONTROL, SUCH AS A PROPRIETARY OPINION COLUMN; OR WHEN THE ISP IS MADE AWARE THAT OFFENDING CONTENT HAS BEEN POSTED ON A WEB SITE IT HOSTS AND DOES NOT REMOVE IT.

TO HOLD ISPS PRESUMPTIVELY LIABLE FOR ALL CONTENT THEY HOST OR CARRY WOULD POSE A REGULATORY BURDEN ON PROVIDERS THAT WOULD DRASTICALLY REDUCE AND SLOW THE FLOW OF INFORMATION—IF THE BURDEN COULD BE CARRIED AT ALL. THE GLOBAL INTERNET LIBERTY CAMPAIGN (GILC) ARGUES, “NO ONE CAN MONITOR THE ENORMOUS QUANTITY OF NETWORK TRAFFIC, WHICH MAY CONSIST OF

⁹ DINAH POKEMPNER, “BRIEFING PAPER: ENCRYPTION IN THE SERVICE OF HUMAN RIGHTS,” AUGUST 1, 1997, <[HTTP://WWW.AAS.ORG/SPP/DSPP/ESTC/BRIEFING/CRYPTO/DINAH.HTM](http://www.aas.org/spp/dspp/estc/briefing/crypto/dinah.htm)>.

HUNDREDS OF THOUSANDS OF E-MAILS, NEWSGROUP MESSAGES, FILES, AND WEB PAGES THAT PASS THROUGH IN DOZENS OF TEXT AND BINARY FORMATS, SOME OF THEM READABLE ONLY BY PARTICULAR PROPRIETARY TOOLS." SECOND, GILC POINTS OUT, "ISPs CANNOT PROVIDE MATERIAL IN ONE COUNTRY WHILE BLOCKING IT IN ANOTHER; SUCH A DISTINCTION WOULD REQUIRE AN ENORMOUS NEW INFRASTRUCTURE ON TOP OF THE CURRENT NETWORK."⁹

⁹ GLOBAL INTERNET LIBERTY CAMPAIGN, *REGARDLESS OF FRONTIERS: PROTECTING THE HUMAN RIGHTS TO FREEDOM OF EXPRESSION ON THE GLOBAL INTERNET* (WASHINGTON, DC: CENTER FOR DEMOCRACY AND TECHNOLOGY, SEPTEMBER 1999), PP. 30-31. GILC IS A COALITION OF ORGANIZATIONS, INCLUDING HUMAN RIGHTS WATCH, THAT SEEKS TO PROMOTE FREE EXPRESSION, PRIVACY, AND OTHER RIGHTS IN ONLINE COMMUNICATIONS. *REGARDLESS OF FRONTIERS* IS ALSO AT <[WWW.GILC.ORG/SPEECH/REPORT](http://www.gilc.org/speech/report)>.

IV. INTRODUCTION

THIS REPORT SURVEYS THE EVOLVING POLICIES OF GOVERNMENTS IN THE MIDDLE EAST AND NORTH AFRICA AFFECTING THE RIGHT OF PERSONS TO RECEIVE AND IMPART INFORMATION THROUGH THE INTERNET. ¹⁰ IT AIMS TO REINFORCE AND EXPAND ONLINE FREEDOMS NOT ONLY BY IDENTIFYING VIOLATIONS OF FREE EXPRESSION RIGHTS THAT HAVE TAKEN PLACE, BUT ALSO BY PROPOSING—AT A TIME WHEN INTERNET LAWS AND POLICIES ARE BEING DEVELOPED—STEPS GOVERNMENTS SHOULD TAKE TO PROTECT AND ENHANCE THE RIGHTS OF ALL PERSONS TO EXCHANGE INFORMATION AND IDEAS FREELY THROUGH THIS MEDIUM.¹¹

¹⁰ THE INTERNET IS A WORLDWIDE NETWORK OF COMPUTER NETWORKS THAT PERMITS ANY TWO COMPUTERS IN THE SYSTEM TO EXCHANGE DATA VIA SUCH MEANS AS ELECTRONIC MAIL ("E-MAIL"), THE WORLD WIDE WEB, NEWSGROUPS (ELECTRONIC "BULLETIN BOARDS"), FILE TRANSFERS, AND REAL-TIME "CHAT ROOMS." WHEN USED IN THIS FASHION, "INTERNET" IS CAPITALIZED; "internet" IN LOWER-CASE REFERS TO A LOCAL NETWORK OF COMPUTERS THAT COMMUNICATE WITH ONE ANOTHER USING A COMMON COMMUNICATIONS PROTOCOL.

¹¹ THIS REPORT BUILDS ON THE FINDINGS OF HUMAN RIGHTS WATCH, "SILENCING THE NET: THE THREAT TO FREEDOM OF EXPRESSION ON-LINE," *A HUMAN RIGHTS WATCH REPORT*, VOL. 9, NO. 2, MAY 1996; AND HUMAN RIGHTS WATCH, "ELECTRIFYING SPEECH: NEW COMMUNICATIONS TECHNOLOGIES AND TRADITIONAL CIVIL LIBERTIES," *A HUMAN RIGHTS WATCH REPORT*, VOL. 4, NO. 5, JULY 1992.

IN A REGION WHERE TORTURE IS COMMONPLACE AND FREE ELECTIONS THE EXCEPTION, THE ISSUE OF INTERNET SPEECH MAY SEEM LOW ON THE HUMAN RIGHTS AGENDA. IT MAY ALSO APPEAR TO BE AN ELITIST CONCERN IN COUNTRIES WHERE ILLITERACY IS RAMPANT AND THE COST OF A PERSONAL COMPUTER AND PERHAPS EVEN A TELEPHONE IS BEYOND THE REACH OF MOST HOUSEHOLDS.

BUT IT IS ARGUABLY IN LESS-DEVELOPED AND IN MORE REPRESSIVE COUNTRIES THAT THE INTERNET CAN HAVE THE GREATEST IMPACT. WHEREVER IT IS ACCESSIBLE, THE INTERNET HAS PROVIDED DRAMATIC NEW POSSIBILITIES FOR PEOPLE TO OBTAIN AND EXCHANGE INFORMATION LOCALLY AND INTERNATIONALLY. IT HAS BEEN HAILED BY MANY AS A FORCE FOR ERODING AUTHORITARIAN POLITICAL CONTROL AND AIDING PARTICIPATORY DEMOCRACY.

AS THE FIRST TRULY "MASS" MEDIUM, ONE THAT IS INHERENTLY OPEN AND DECENTRALIZED, THE INTERNET CAN ENABLE ANYONE TO RECEIVE AND TO DISSEMINATE ALTERNATIVES TO STATE-CONTROLLED INFORMATION AT A LOW COST. WHILE FEW INDIVIDUALS AND GROUPS HAVE THE MEANS TO PUBLISH BOOKS OR NEWSPAPERS, MAKE A FILM, OR AIR A RADIO OR TELEVISION PROGRAM, ANY PERSON WITH ACCESS TO A PERSONAL COMPUTER AND MODEM CAN COMMUNICATE WITH A HUGE INTERNATIONAL AUDIENCE. A CONNECTION TO THE INTERNET CAN INCREASE ACCESS TO INFORMATION IN LESS-DEVELOPED COUNTRIES BY PUTTING WITHIN EASY REACH ONE OF THE WORLD'S GREAT REPOSITORIES OF INFORMATION, MUCH OF IT FREE AND CONTINUOUSLY UPDATED, AND BY MAKING THAT INFORMATION MORE EASILY MANAGEABLE AND TRANSFERABLE.

SUCH BENEFITS DO NOT DEPEND ON A LARGE NUMBER OF PERSONS HAVING THE MEANS TO PURCHASE THEIR OWN EQUIPMENT AND INTERNET ACCOUNTS. A GOVERNMENT POLICY OF MAKING COMPUTERS AVAILABLE TO THE PUBLIC AT LIBRARIES, SCHOOLS OR COMMUNITY CENTERS, OR THE PRESENCE OF PRIVATELY RUN "INTERNET CAFÉS" OR "CYBERCAFÉS" (SHOPS OFFERING THE PUBLIC FEE-FOR-USE INTERNET ACCESS), CAN HELP TO DEMOCRATIZE USE OF THE INTERNET EVEN IN RELATIVELY POOR COUNTRIES.

IN LIGHT OF THE INTERNET'S VAST POTENTIAL FOR EMPOWERING PEOPLE TO EXERCISE THE RIGHT TO FREE EXPRESSION, SOME HAVE ARGUED THAT GOVERNMENTS HAVE AN AFFIRMATIVE OBLIGATION TO FACILITATE INTERNET ACCESS FOR ALL SEGMENTS OF THE POPULATION ON TERMS OF NONDISCRIMINATION. SOME HAVE ALSO CONTENDED THAT THE INTERNET CAN SIGNIFICANTLY ASSIST GOVERNMENTS IN ENABLING CITIZENS TO EXERCISE THE RIGHT, UNDER ARTICLE 25(A) OF THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS, "TO TAKE PART IN THE CONDUCT OF PUBLIC AFFAIRS, DIRECTLY OR THROUGH FREELY CHOSEN REPRESENTATIVES." THE EXERCISE OF THIS RIGHT IS ENHANCED BY PROVIDING CITIZENS ACCESS TO ALL DRAFT AND EFFECTIVE LAWS, TRANSCRIPTS OF PARLIAMENTARY DEBATES, AND OTHER INFORMATION RELEVANT TO CIVIC AFFAIRS. AS THE GLOBAL INTERNET LIBERTY CAMPAIGN (GILC) NOTES, "IN ALMOST EVERY COUNTRY IN THE WORLD, MOST GOVERNMENT INFORMATION IS NOW CREATED BY WORD PROCESSING, MEANING THAT THE INFORMATION IS ALREADY DIGITIZED...[AND] CAN BE RAPIDLY AND INEXPENSIVELY PUT ON-LINE, EVEN USING SIMPLE GOPHER TECHNOLOGY."¹²

THE INTERNET'S POTENTIAL CONTRIBUTION TO DEMOCRATIC AND PARTICIPATORY POLITICS IS GAINING RECOGNITION. IN HIS 1999 REPORT TO THE U.N. COMMISSION ON HUMAN RIGHTS, THE SPECIAL RAPPORTEUR

¹² REGARDLESS OF FRONTIERS, PP. 7-9.

ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION OUTLINED THE CASE AGAINST GOVERNMENT REGULATION OF INTERNET ACCESS AND CONTENT AS FOLLOWS:

[T]HE NEW TECHNOLOGIES AND, IN PARTICULAR, THE INTERNET, ARE INHERENTLY DEMOCRATIC, PROVIDE THE PUBLIC AND INDIVIDUALS WITH ACCESS TO INFORMATION AND SOURCES AND ENABLE ALL TO PARTICIPATE ACTIVELY IN THE COMMUNICATION PROCESS. THE SPECIAL RAPPORTEUR ALSO BELIEVES THAT ACTION BY STATES TO IMPOSE EXCESSIVE REGULATIONS ON THE USE OF THESE TECHNOLOGIES AND, AGAIN, PARTICULARLY THE INTERNET, ON THE GROUNDS THAT CONTROL, REGULATION AND DENIAL OF ACCESS ARE NECESSARY TO PRESERVE THE MORAL FABRIC AND CULTURAL IDENTITY OF SOCIETIES IS PATERNALISTIC. THESE REGULATIONS PRESUME TO PROTECT PEOPLE FROM THEMSELVES AND, AS SUCH ARE INHERENTLY INCOMPATIBLE WITH THE PRINCIPLES OF THE WORTH AND DIGNITY OF EACH INDIVIDUAL.¹³

INTERNET CONNECTIVITY IS OF SPECIAL SIGNIFICANCE TO CIVIL SOCIETY. COMPUTER NETWORKS FILL A "MEDIA GAP" BETWEEN INTERPERSONAL COMMUNICATION FACILITATED BY TELEPHONE, TELEGRAM, AND LETTERS, AND MASS COMMUNICATION FACILITATED BY RADIO, TELEVISION, AND PRINT MEDIA.¹⁴ COMPUTER NETWORKS CAN GREATLY FACILITATE SMALL-GROUP PARTICIPATION—WITHIN GROUPS, BETWEEN GROUPS,

¹³ UNITED NATIONS ECONOMIC AND SOCIAL COUNCIL, "REPORT OF THE SPECIAL RAPPORTEUR, MR. ABID HUSSAIN, SUBMITTED PURSUANT TO COMMISSION ON HUMAN RIGHTS RESOLUTION 1997/26" (NEW YORK: UNITED NATIONS, 1999), E/CN.4/1999/40.

¹⁴ SEE ANDREA KAVANAUGH, *THE SOCIAL CONTROL OF TECHNOLOGY IN NORTH AFRICA: INFORMATION IN THE GLOBAL ECONOMY* (WESTPORT, CONNECTICUT: GREENWOOD, 1999), P. 5.

AND BETWEEN GROUPS AND THEIR CONSTITUENCIES—AND THUS HELP TO STRENGTHEN THE FORCES OF CIVIL SOCIETY. MANY HUMAN RIGHTS ORGANIZATIONS HAVE EMBRACED THE INTERNET AS A MEANS OF EXCHANGING INFORMATION QUICKLY AND CHEAPLY.¹⁵ GROUPS IN THE MIDDLE EAST AND NORTH AFRICA HAVE PROVED NO EXCEPTION TO THIS TREND.¹⁶

IN PREPARING THIS REPORT, HUMAN RIGHTS WATCH SENT A UNIFORM LETTER TO THE GOVERNMENTS OF MOROCCO, ALGERIA, TUNISIA, LIBYA, EGYPT, ISRAEL, THE PALESTINIAN AUTHORITY, LEBANON, JORDAN, SYRIA, IRAQ, KUWAIT, THE UNITED ARAB EMIRATES, SAUDI ARABIA, QATAR, OMAN, AND YEMEN. IN MOST INSTANCES, THE LETTER WAS SENT TO MORE THAN ONE OFFICIAL ADDRESS, AND FOLLOWED UP WITH PHONE CALLS OR FAXES. THE LETTER CONTAINED A SERIES OF QUESTIONS ABOUT INTERNET POLICIES. IT IS REPRINTED IN APPENDIX B. WRITTEN RESPONSES WERE RECEIVED FROM THE GOVERNMENTS OF JORDAN, TUNISIA, YEMEN, AND IRAQ. THE GOVERNMENTS OF MOROCCO, KUWAIT, QATAR, AND THE UNITED ARAB EMIRATES FURNISHED LIMITED INFORMATION ABOUT THE INTERNET IN THEIR COUNTRIES. ALGERIA, SAUDI ARABIA, LIBYA, EGYPT, ISRAEL, LEBANON, SYRIA, SAUDI ARABIA, AND OMAN PROVIDED NO ANSWER WHATSOEVER; THE PALESTINIAN AUTHORITY ACKNOWLEDGED RECEIPT OF HUMAN RIGHTS WATCH'S LETTER BUT DID NOT RESPOND TO ITS CONTENT. THE OFFICIAL RESPONSES TO THE HUMAN RIGHTS WATCH LETTER HAVE BEEN EXCERPTED BELOW IN THE COUNTRY PROFILES SECTION AND REPRINTED IN APPENDIX C.

THE COUNTRY PROFILES SECTION OF THIS REPORT DESCRIBES GOVERNMENT POLICIES AFFECTING ONLINE FREEDOM OF EXPRESSION IN EIGHT COUNTRIES. AS THE FIRST STUDY OF THIS SUBJECT BY HUMAN RIGHTS WATCH'S MIDDLE EAST AND NORTH AFRICA DIVISION, THIS REPORT IS BY NO MEANS A COMPREHENSIVE SURVEY OF ONLINE EXPRESSION ISSUES IN ANY ONE COUNTRY OR IN THE REGION AS A WHOLE. WE HOPE TO EXPAND OUR INFORMATION BASE AND TO KEEP IT UP-TO-DATE, AND WELCOME QUERIES AND COMMENTS SENT TO:

¹⁵ A USEFUL RESOURCE IS STEPHEN A. HANSEN, *GETTING ONLINE FOR HUMAN RIGHTS: FREQUENTLY ASKED QUESTIONS AND ANSWERS ABOUT USING THE INTERNET IN HUMAN RIGHTS WORK* (WASHINGTON, D.C.: AMERICAN ASSOCIATION FOR THE ADVANCEMENT OF SCIENCE, 1999). THE FULL TEXT OF THE PRINTED VERSION CAN BE FOUND AT <[HTTP://SHR.AABS.ORG/ONLINE/COVER.HTM](http://shr.aabs.org/online/cover.htm)>.

¹⁶ SEE NANCY GALLAGHER, "MIDDLE EAST AND NORTH AFRICA HUMAN RIGHTS ACTIVISM IN CYBERSPACE," *MIDDLE EAST STUDIES ASSOCIATION BULLETIN*, VOL. 31, NO. 1, JULY 1997, <[HTTP://WFP.ARIZONA.EDU/MESASSOC/BULLETIN/GALLEGH.HTM](http://wfp.arizona.edu/mesassoc/bulletin/gallagh.htm)>.

HUMAN RIGHTS WATCH
MIDDLE EAST AND NORTH AFRICA DIVISION
1630 CONNECTICUT AVENUE, NW, FIFTH FLOOR
WASHINGTON, DC 20009 USA
FAX (202)612-4333
HRWDC@HRW.ORG

V. THE INTERNET IN THE MIDDLE EAST AND NORTH AFRICA: A CAUTIOUS START

THE MIDDLE EAST AND NORTH AFRICA IS ONE OF THE MOST UNDER-REPRESENTED AREAS OF THE WORLD IN TERMS OF PER CAPITA INTERNET CONNECTIVITY. IN A REGION WHERE NEARLY EVERY GOVERNMENT CENSORS OR PUNISHES SPEECH CRITICAL OF THE AUTHORITIES,¹⁷ THERE CAN BE LITTLE DOUBT THAT INTERNET GROWTH HAS BEEN SLOWED BY THE FEAR AMONG THOSE IN POWER THAT DEMOCRATIZING INTERNET ACCESS WILL UNDERMINE STATE CONTROL OVER INFORMATION. SAUDI AUTHORITIES STATED BLUNTLY DURING 1998 THAT THE CONTINUING DELAYS IN OPENING THE INTERNET TO PUBLIC ACCESS WERE DUE TO THE SEARCH FOR A SYSTEM BY WHICH AUTHORITIES COULD BLOCK THE FLOW OF "UNDESIRABLE" INFORMATION.

BUT AFTER A SLOW START, THE SPREAD OF THE INTERNET IN THE REGION HAS ACCELERATED OVER THE LAST FOUR YEARS. PRO-INTERNET FORCES WITHIN GOVERNMENTS AND IN THE BUSINESS, ACADEMIC, AND RESEARCH COMMUNITIES, WISHING TO KEEP CURRENT AND GLOBALLY COMPETITIVE, HAVE PUSHED FOR EASIER ACCESS TO ONLINE DATA AND COMMUNICATIONS.

AS OF MAY 1999, EVERY COUNTRY IN THE REGION EXCEPT IRAQ AND LIBYA HAD SOME FORM OF INTERNATIONAL CONNECTIVITY. MEMBERS IN ALL OF THESE COUNTRIES EXCEPT SYRIA COULD CONNECT TO THE INTERNET IN SOME FASHION VIA LOCAL INTERNET SERVICE PROVIDERS (ISPs).¹⁸

¹⁷ FOR COUNTRY-BY-COUNTRY COVERAGE OF PRESS RESTRICTIONS, SEE THE REGULARLY UPDATED REPORTS OF THE COMMITTEE TO PROTECT JOURNALISTS (<www.cpj.org/countrystatus>), REPORTERS SANS FRONTIÈRES (<www.rsf.fr>), HUMAN RIGHTS WATCH (<www.hrw.org>), AND THE U.S. STATE DEPARTMENT'S COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES (<www.state.gov/www/global/human_rights/hrp_reports_mainhp.html>).

¹⁸ AN ISP IS A COMPANY THAT PROVIDES INTERNET ACCOUNTS, CONNECTIONS, AND SERVICES TO INDIVIDUALS AND/OR BUSINESSES.

At that time, there were an estimated 990,000 persons "online" in the Middle East, including Israel but excluding North Africa, according to NVA, a Dublin-based information technology firm (see table in Appendix A).¹⁹ In at least fourteen countries (Morocco, Algeria, Tunisia, Egypt, Israel, the Palestinian self-rule areas, Lebanon, Jordan, Kuwait, Bahrain, Qatar, Iran, Oman, and the United Arab Emirates) cybercafés afforded the public access to the Internet for an hourly fee.²⁰

The Arab press avidly follows Internet news, and conferences on the information revolution have become commonplace in the region. For example, Syria—which has yet to allow

¹⁹ NVA's surveys, at <www.nva.ie/surveys/how_many_online>, are regularly updated. Its Middle East survey draws heavily on information collected by another company based in the United Arab Emirates, the Dabbagh Information Technology Group (<www.dit.net>). NVA cautions that the surveys are imprecise.

²⁰ When visited on May 12, 1999, the web site <www.netcafeguide.com> provided a noncomprehensive list of fifty-three cybercafés in the Middle East and North Africa. For a profile of the first cybercafé to open in Iran, see Mike Theodoulou, "The Imams Are Wrestling with the Internet in the Battle for Nation's Young Minds," *THE TIMES* (London), April 17, 1999, and Christophe de Roquefeuil, "Islam on Line et Croissants," *LIBÉRATION*, December 10, 1999. On the first cybercafé in Algeria, see Cherif Ouazani, "Bob El Web City," *JEUNE AFRIQUE*, August 4, 1999. For a commentary by a Yemeni journalist decrying the absence of cybercafés in that country, see Walid al-Saqqa, "How to Upgrade Use of the Internet," *YEMEN TIMES*, February 1, 1999, <www.yementimes.com/99/ISS05/TECHNO.HTM>.

INTERNET ACCESS TO THE PUBLIC—HOSTED THE “SECOND AL-SHAAM INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY” IN DAMASCUS IN APRIL 1999.²¹ ANOTHER INDICATION OF INTERNET GROWTH IS THE PUBLICATION IN 1999 OF A COMMERCIAL YELLOW-PAGES, THE MIDDLE EAST INTERNET DIRECTORY: A COMPREHENSIVE GUIDE TO MIDDLE EAST WEB SITES (<[HTTP://MIDDLEEASTDIRECTORY.COM](http://MiddleEastDirectory.com)>).

THE FOLLOWING EXAMPLES DEMONSTRATE HOW THE INTERNET IS EMPOWERING CITIZENS AND NONGOVERNMENTAL FORCES, AND ERODING GOVERNMENT-IMPOSED CONTROLS ON THE FLOW OF INFORMATION:

- THROUGH E-MAIL AND WEB SITES, HUMAN RIGHTS ORGANIZATIONS IN EGYPT, THE PALESTINIAN TERRITORIES, AND ELSEWHERE DISSEMINATE INFORMATION FAR MORE EFFECTIVELY THAN EVER BEFORE, DESPITE THEIR MODEST RESOURCES AND LIMITED ACCESS TO THE LOCAL MEDIA.²²

²¹ “SYRIAN CONFERENCE CALLS FOR WIDER INTERNET ACCESS,” REUTERS, MAY 1, 1999.

²² SEE GALLAGHER, “MIDDLE EAST AND NORTH AFRICA HUMAN RIGHTS ACTIVISM IN CYBERSPACE” AND DEBORAH WHEELER, “IN PRAISE OF THE VIRTUAL LIFE: NEW COMMUNICATIONS TECHNOLOGIES, HUMAN RIGHTS, DEVELOPMENT, AND THE DEFENSE OF MIDDLE EASTERN CULTURAL SPACE” <[WWW.CWRL.UTEXAS.EDU/~MONITORS/1.1/WHEELER/INDEX.HTML](http://www.cwrl.utexas.edu/~monitors/1.1/wheeler/index.html)>. THE WEB SITE ON WHICH THIS ARTICLE APPEARS IS ENTITLED *Monitors: A Journal of Human Rights and Technology*.

- ARABIC, ENGLISH, AND FRENCH NEWSPAPERS THAT HAVE BEEN CENSORED IN EGYPT, ALGERIA AND JORDAN HAVE POSTED THEIR BANNED STORIES ONLINE, WHERE LOCAL AND INTERNATIONAL READERS CAN VIEW THEM. STORIES THAT NEWSPAPERS DECLINED TO PUBLISH, DUE TO POLITICAL PRESSURE OR OTHER FACTORS, HAVE CIRCULATED WIDELY ON THE INTERNET.²³ WHEN PRIVATE DAILIES IN ALGERIA WENT ON STRIKE IN OCTOBER 1999 TO PROTEST PRESSURE FROM STATE-RUN PRINTING PRESSES, THEY PUBLISHED BULLETINS DAILY ON THE WEB TO MOBILIZE SUPPORT FOR THEIR CAUSE.²⁴ INTERNET-BASED ORGANIZATIONS LIKE THE DIGITAL FREEDOM NETWORK (<www.dfn.org>) HAVE BEEN MAKING CENSORED MATERIALS AVAILABLE ONLINE. DURING 1999, THE DFN POSTED ARTICLES THAT HAD BEEN BANNED BY AUTHORITIES IN EGYPT, MAURITANIA, TUNISIA, AND TURKEY.

²³ *AL-Quds AL-Arabi* was banned from entering Jordan on May 19, 1999. The London-based daily then took out advertisements in Jordanian newspapers directing readers to its online edition at <www.alquds.co.uk>. When Egyptian censors excised articles from the Nicosia-based *Middle East Times*, readers could view the censored material at the web site of the English-language weekly, <www.metimes.com>. In Algeria, journalists at the much-censored *La Nation* were able to post an edition of the weekly at the web site of Reporters sans Frontières, a French freedom of expression organization, after *La Nation* closed its doors in 1996 (<www.rsf.fr/censure/datibao/index.html>).

²⁴ A writer at the Algiers-based French-language daily *El-Watan* wrote, "Sending out via the Internet special editions of the main private newspapers, which have been on strike for ten days, makes it possible to target a readership that follows what is happening in Algeria. Netsurfers, mostly Algerians who are dispersed throughout the world, can read in real time information that is addressed to them. This decision, made deliberately by editors who denounce the political pressures by the authorities, is a first. The World Wide Web is becoming indispensable. "La Presse Libre sur le Web," October 27, 1999.

- CITIZENS OF ARAB COUNTRIES HAVE DEBATED AND CONVERSED WITH ISRAELIS IN "CHAT ROOMS" AND OTHER ONLINE FORUMS AT A TIME WHEN IT IS DIFFICULT OR IMPOSSIBLE FOR THEM TO HAVE FACE-TO-FACE CONTACT, TELEPHONE CONVERSATIONS, AND POSTAL CORRESPONDENCE, DUE TO TRAVEL RESTRICTIONS AND THE ABSENCE OF PHONE OR MAIL LINKS BETWEEN MOST ARAB COUNTRIES AND ISRAEL.
- MOROCCANS CAN FIND COPIOUS INFORMATION POSTED ON THE WEB BY THE POLISARIO FRONT AND OTHERS WHO CHALLENGE THE OFFICIAL MOROCCAN LINE ON THE WESTERN SAHARA (SEE, FOR EXAMPLE, <www.arsso.org>). SUCH INFORMATION IS EITHER NONEXISTENT OR ONE-SIDED IN THE LOCAL NEWS MEDIA, BOOKSHOPS, AND LIBRARIES.
- ALGERIANS CAN VISIT NUMEROUS WEB SITES MOUNTED BY ISLAMIST GROUPS THAT ARE BANNED AND HAVE NO LEGAL PUBLICATIONS INSIDE ALGERIA, INCLUDING THE FRONT ISLAMIQUE DU SALUT (<www.fisalgeria.org>).²⁵
- AN ARAB GAY AND LESBIAN WEB SITE (<www.glas.org>) CATERS TO PEOPLE WHO, IN MANY ARAB COUNTRIES, HAVE FEW PLACES TO GO TO OBTAIN INFORMATION PERTAINING TO THEIR SEXUAL ORIENTATION.
- THE WORLD WIDE WEB, WITH ITS ONLINE NEWSPAPERS AND RADIO AND TV WEBCASTING, HAS DRAMATICALLY ENHANCED THE DIVERSITY OF NEWS AVAILABLE TO PEOPLE IN THE MIDDLE EAST. (SO HAVE THE IMMENSELY POPULAR ARABIC-LANGUAGE SATELLITE TELEVISION STATIONS.²⁶) THE CHANGE IS ESPECIALLY MARKED FOR THOSE LIVING IN COUNTRIES WHERE FOREIGN NEWSPAPERS ARE EITHER UNAVAILABLE, EXPENSIVE, OR OUT-OF-DATE WHEN THEY ARRIVE.

MOST COUNTRIES THAT HAVE ALLOWED INTERNET ACCESS HAVE TOLERATED FREER EXPRESSION ONLINE THAN IS PERMITTED IN THE LOCAL NEWS MEDIA. KUWAIT, MOROCCO, ALGERIA, EGYPT, JORDAN, AND LEBANON

²⁵ ON ALGERIA, SEE CHRISTOPHE LOBBÉ AND OLIVIA RECASENS, "INTERNET DONNE LA PAROLE AUX ALGÉRIENS," *LE MONDE*, MARCH 22, 1999.

²⁶ SEE JON B. ALTERMANN, *NEW MEDIA, NEW POLITICS? FROM SATELLITE TELEVISION TO THE INTERNET IN THE ARAB WORLD* (WASHINGTON, DC: THE WASHINGTON INSTITUTE FOR NEAR EAST POLICY, 1999).

HAVE ALL PERMITTED RELATIVELY UNFETTERED ONLINE SPEECH FOR THE THOUSANDS OF USERS IN EACH COUNTRY, EVEN AS THEY ENFORCE PRESS LAWS AGAINST PRINT PERIODICALS THAT PUBLISH "OBJECTIONABLE" MATERIAL.

THE EXTENT OF INTERNET CONNECTIVITY IN A COUNTRY IS DETERMINED BY MANY FACTORS IN ADDITION TO GOVERNMENT POLICIES TOWARD FREEDOM OF INFORMATION AND EXPRESSION. THESE INCLUDE THE AFFORDABILITY TO THE PUBLIC OF COMPUTER EQUIPMENT AND OF INTERNET AND PHONE CONNECTIONS, AND THE STATE OF A COUNTRY'S TELECOMMUNICATIONS INFRASTRUCTURE, INCLUDING SUCH ATTRIBUTES AS THE NUMBER OF TELEPHONE LINES PER CAPITA²⁷ AND THE INTERNATIONAL CONNECTION'S BANDWIDTH.²⁸

²⁷ FOR COUNTRY-BY-COUNTRY STATISTICS ON TELEPHONES AND COMPUTERS, SEE THE WORLD BANK, *WORLD DEVELOPMENT REPORT: KNOWLEDGE FOR DEVELOPMENT, 1999/99* (OXFORD: OXFORD UNIVERSITY PRESS, PUBLISHED FOR THE WORLD BANK, 1999), PP. 226-227.

²⁸ BANDWIDTH IS THE AMOUNT OF DATA THAT CAN FLOW OVER A NETWORK IN A FIXED AMOUNT OF TIME. "LOW BANDWIDTH MEANS SLOW, EVEN EXCRUCIATINGLY SLOW, CONNECTIONS TO THE INTERNET WHICH MATTER MORE WITH THE MORE ADVANCED USES SUCH AS THE WORLD WIDE WEB, ESPECIALLY UNDER A UNIT-PRICING REGIME [I.E., A SLOW BANDWIDTH WILL REQUIRE LONGER ONLINE TIME TO PERFORM THE SAME TASKS, THUS HIKING COSTS FOR USERS WHO PAY FOR THEIR PHONE SERVICE BY TIME SEGMENTS]. THE WEB IS OPTIMIZED FOR DIRECT CONNECTION TO THE INTERNET SUCH AS THROUGH A UNIVERSITY OR CORPORATE NETWORK. THE MORE MULTIMEDIA IT BECOMES, WITH GRAPHICS, ANIMATION, SOUND, EVEN VIDEO-CONFERENCING, THE GREATER ITS BANDWIDTH DEMANDS. SO THE LOW BANDWIDTH IN MIDDLE EAST LOCAL SERVICES AND THE HIGH COST OF INTERNATIONAL TELEPHONE CALLS CHARGED BY MIDDLE EASTERN TELECOMMUNICATION UTILITIES DISCOURAGE WEB USE, WHICH IS RARER IN THE REGION THAN E-MAIL AND DISCUSSION GROUPS." JON ANDERSON, "THE INTERNET AND THE MIDDLE EAST: COMMERCE BRINGS REGION ON-LINE," *MIDDLE EAST EXECUTIVE REPORTS*, VOL. 20, NO. 12, DECEMBER 1997, <[WWW.GEORGETOWN.EDU/RESEARCH/BRABTECH/MEER97.HTM](http://www.georgetown.edu/research/brabtech/meer97.htm)>.

IN MOST COUNTRIES OF THE WORLD THAT HAVE KNOWN RAPID INTERNET GROWTH, THE PUBLIC SECTOR HAS PLAYED A ROLE BY, AMONG OTHER THINGS, BUILDING "BACKBONE" TELECOMMUNICATIONS NETWORKS, PROVIDING INITIAL FUNDING, REGULATIONS, AND STANDARDS, AND BY ENCOURAGING PRIVATE INVESTMENT AND COMPUTER LITERACY. THUS, GOVERNMENTS THAT FAVOR DEVELOPMENT OF THE INTERNET MUST ADOPT AFFIRMATIVE POLICIES, AND NOT SIMPLY REFRAIN FROM CENSORSHIP AND RESTRICTING ACCESS. FEW GOVERNMENTS IN THE MIDDLE EAST AND NORTH AFRICA HAVE EMBRACED SUCH AN APPROACH. THE REASONS INCLUDE COMPETING DEMANDS FOR SCARCE STATE RESOURCES, FEAR OF LOSING CONTROL OVER INFORMATION, AND A DESIRE TO PROTECT MONOPOLY PROFITS OF STATE TELECOMMUNICATIONS COMPANIES.²⁹ CHAKIB LAHRICHI, PRESIDENT OF THE INDEPENDENT INTERNET ASSOCIATION IN MOROCCO, STATED THAT WHILE THE MOROCCAN GOVERNMENT HAD NO EXPLICIT POLICY OF CENSORING OR RESTRICTING ACCESS TO THE INTERNET, ITS GROWTH HAD BEEN STUNTED BY UNFAIR ADVANTAGES ENJOYED BY THE STATE-CONTROLLED TELECOMMUNICATIONS COMPANY HISSALAT AL-MAGHRIB IN ITS COMPETITION WITH PRIVATE SERVICE PROVIDERS, ALONG WITH THE GOVERNMENT'S FAILURE TO EDUCATE THE PUBLIC ABOUT THE INTERNET.³⁰

THE LOCAL PRICES OF COMPUTER EQUIPMENT OR SERVICES ALSO DETER INTERNET USE IN MANY COUNTRIES OF THE REGION. THOSE PRICES MAY REFLECT GOVERNMENT ATTITUDES TOWARD POPULARIZING INTERNET USE, INsofar AS THOSE PRICES ARE SET, TAXED OR SUBSIDIZED BY THE GOVERNMENT. THROUGHOUT THE REGION, INTERNET AND TELEPHONE COSTS ARE MORE EXPENSIVE THAN THEY ARE, FOR EXAMPLE, IN THE UNITED STATES. THEY ARE EVEN MORE COSTLY WHEN PREVAILING MEDIAN INCOME LEVELS ARE TAKEN INTO CONSIDERATION.

ANOTHER FACTOR INHIBITING INTERNET GROWTH IN THE REGION IS THE CONTINUING DOMINANCE OF ENGLISH-LANGUAGE MATERIALS. ALTHOUGH THE VOLUME OF MATERIAL IN ARABIC IS GROWING AND THE ARABIC SOFTWARE AVAILABLE FOR BROWSING THE WEB IS IMPROVING,³¹ USERS WHO DO NOT SPEAK ENGLISH REMAIN AT A DISADVANTAGE IN THEIR ABILITY TO ACCESS ONLINE RESOURCES.³² FRENCH SPEAKERS, SUCH AS

²⁹ ON THE OFTEN REGRESSIVE ROLE OF TELECOMMUNICATION MONOPOLIES, SEE MUHAMMAD ARIF, "AL-MUSTAQBAL LI HAFIF AL-INTERNET ELETHI YADKHAL AL-MANTAQA AL-'ARABIYYA BI-HATHIR," ("THE FUTURE OF INTERNET LINES THAT ARE CAUTIOUSLY COMING TO THE ARAB WORLD"), *AL-HAYAT* (LONDON), JULY 9, 1999, AND DAVID BUTTER, "TELECOMS REFORM TAKES THE LEAD," *MIDDLE EAST ECONOMIC DIGEST*, MAY 9, 1999, PP. 2-3.

³⁰ INTERVIEW, CASABLANCA, APRIL 30, 1999, AND E-MAIL COMMUNICATION FROM LAHRICHI TO HUMAN RIGHTS WATCH, MAY 12, 1999.

³¹ THE FACT THAT, INITIALLY, MUCH OF THE ARABIC MATERIALS THAT WERE POSTED ON THE WEB WERE POSTED AS GRAPHIC FILES RATHER THAN AS TEXT FILES MEANT THAT THEY DID NOT LEND THEMSELVES TO TEXT SEARCHES, A KEY ADVANTAGE OF HANDLING CONTENT ONLINE.

³² SURVEYS OF THE PRESENCE OF LANGUAGES ON THE WEB INDICATE THAT MATERIALS IN ENGLISH ACCOUNT FOR MORE THAN 90 PERCENT OF CONTENT, ALTHOUGH THAT DOMINANCE SEEMS TO BE DECLINING. SEE, FOR EXAMPLE, "WEB LANGUAGES HIT PARADE," JUNE 1997 (<<http://babel.alis.com:9090/palmares.en.html>>), COMPILED BY THE BABEL TEAM, A JOINT INITIATIVE OF ALIS TECHNOLOGIES AND THE INTERNET SOCIETY. ARABIC MATERIAL ACCOUNTS FOR ONLY A TINY FRACTION OF THE REMAINDER. SEE "EXPERT CALLS FOR PROMOTION OF ARABIC ON INTERNET," *XINHUA NEWS*

MANY NORTH AFRICANS, HAVE ACCESS TO SIGNIFICANTLY MORE MATERIALS THAN DO MONOLINGUAL ARABIC SPEAKERS.

SOME SOCIAL FORCES HAVE VOICED HOSTILITY TO THE INTERNET OR TO ITS AVAILABILITY TO THE PUBLIC AT LARGE. LEGISLATORS IN KUWAIT, ISRAEL AND ELSEWHERE HAVE DENOUNCED THE INTERNET AS A THREAT TO LOCAL CULTURE, MORALS, OR RELIGIOUS SENSIBILITIES. IN IRAN, THE CLERICAL MONTHLY *SOBH* CALLED FOR A BAN ON THE INTERNET.³³

AGENCY, DECEMBER 30, 1998.

³³ NEIL MACFARQUHAR, "WITH MIXED FEELINGS, IRAN TIPS TOES TO THE INTERNET," *THE NEW YORK TIMES*, OCTOBER 9, 1996.

GOVERNMENTS AND THEIR SUPPORTERS HAVE SOUNDED THESE THEMES TO JUSTIFY A GO-SLOW, PATERNALISTIC APPROACH TO ALLOWING PUBLIC ACCESS TO THE INTERNET. FOR EXAMPLE, THE SPOKESMAN OF THE SYRIAN COMPUTER SOCIETY, WHICH IS CHAIRED BY THE SON OF PRESIDENT HAFEZ AL-ASAD, WAS QUOTED AS SAYING, "OUR PROBLEM IS...WE ARE A TRADITIONAL SOCIETY AND WE HAVE TO KNOW IF THERE IS SOMETHING THAT CANNOT FIT WITH OUR SOCIETY. WE HAVE TO MAKE IT SAFE."⁵⁴

SIMILAR ARGUMENTS HAVE BEEN MADE BY SAUDIS. SALEH ABDULRAHMAN AL-'ADHEL, THE HEAD OF THE KING ABDUL-AZIZ CITY FOR SCIENCE AND TECHNOLOGY (KACST), REPORTEDLY STATED THAT THE INTERNET PRESENTS "AN IMPORTANT SERVICE IN RELAYING AND DISTRIBUTING INFORMATION BUT ALSO HAS A NEGATIVE SIDE THAT CONFLICTS WITH OUR FAITH AND OUR ARAB MUSLIM TRADITIONS."⁵⁵ THE CHAIR OF THE SAUDI TECHNOLOGY COMPANY SILKINET, EXPLAINING DELAYS IN ALLOWING LOCAL INTERNET ACCESS, STATED, "EFFORTS ARE ONGOING TO PROVIDE THE BEST OF MODERN TECHNOLOGY, WHILE ENSURING THAT THIS DOES NOT CONFLICT WITH THE TRADITIONS AND CULTURE OF THE REGION."⁵⁶

⁵⁴ JACK REDDEN, "INTERNET ARRIVES IN SYRIA, BUT NOT WITHOUT LIMITS," REUTERS, JULY 10, 1999. AN E-MAIL SENT BY HUMAN RIGHTS WATCH TO THE SCS SEEKING COMMENT ON THE REUTERS STORY WENT UNANSWERED.

⁵⁵ ASSOCIATED PRESS, MAY 12, 1997.

⁵⁶ "LEERY SAUDIS GET WIRED," REUTERS, MAY 6, 1999.

While sites of Western origin still dominate the Internet, many advocates of Islam and Islamism have embraced the Internet as a means of projecting their message. Of all the region's political opposition forces, Islamists are among the most active online, thanks partly to a large number of computer-literate activists living in Europe and North America. At an international meeting in July 1999 in Cairo, Islamic organizations and personalities vowed to use the new information technologies to enhance the image of Islam.³⁷ The Islamic Society of North America scheduled for May 1999 a conference devoted to using the Internet "as a tool for effective presentation of knowledge on Islam" (see <www.islamicinternet.org>). In Iran, an official announced in June 1999 that the complete works of the late Ayatollah Ruhollah Khomeini would soon be available online in various languages.³⁸ A computer institute in the city of Qom was preparing 2,000 Islamic instructional documents for presentation on the Web. The institute's director, Sheikh Ali Korani, defended the Internet thus: "Many things have...a double nature and the Internet is one of them," he explained. "You can use it in different ways. The main thing is to use it for the good. And at present our clergy have not said that it is forbidden."³⁹

No Middle East or North African government, not even the warriest, today wishes to be seen as anti-Internet. Syrian and Saudi officials assured their citizenry that the public would soon have access to the Internet, even as they invoked social conservatism to justify a gradual approach. The official *Tishrin* daily of January 27, 1997 reported that Internet subscriptions

³⁷ Muhammad Salah, "Al-Azhar wa al-Jama'at al-Islamiyya yatanafasan 'ala al-Internet," ("Al-Azhar and the Islamic Group compete on the Internet") *al-Hayat*, July 29, 1999. See also "Egypt's Moslem authorities to launch Islamic web site," *Agence France-Presse*, July 15, 1999.

³⁸ "Iran to put Khomeini's complete works on Internet," *Agence France-Presse*, June 1, 1999.

³⁹ "Islam, Iran and the Internet," CNN Interactive (<www.cnn.com/WORLD/9705/22/iran.tech/index.html>), May 22, 1997.

would be open to the Syrian public in six months, according to a dispatch the same day from United Press International. Twenty-eight months later, press reports from Syria continued to forecast that public Internet access would soon be available. In Saudi Arabia, *al-Jazira* newspaper reported on May 12, 1997 that King Fahd had agreed in principle to allow public access. It was not until January 1999 that local ISPs were allowed to serve ordinary citizens—almost five years after state institutions were first linked to the Internet. The long wait was necessary to “finalize the technology needed to bar access to information which is contrary to our Islamic values and dangerous to our security,” explained the head of a group studying the issue at Riyadh’s Chamber of Commerce and Industry.⁴⁰

⁴⁰ Habib Trabelsi, “Saudi’s Near End of Seven-Year Wait to Surf the Net,” *Agence France-Presse*, July 15, 1999.

REGULATORS AROUND THE WORLD ARGUE THAT CURBS ON FREEDOM OF EXPRESSION ON THE INTERNET ARE NEEDED TO PROTECT CHILDREN FROM HARMFUL CONTENT, PRESERVE RELIGIOUS VALUES, SAFEGUARD LOCAL CULTURES, PROTECT NATIONAL SECURITY, THWART TERRORISTS, AND SILENCE RACISTS. IN THE MIDDLE EAST AND NORTH AFRICA, FEW OFFICIALS WILL ADMIT THAT BLOCKING UNWELCOME POLITICAL INFORMATION IS AMONG THEIR OBJECTIVES IN IMPOSING CONTROLS ON THE INTERNET. IN THE PERSIAN GULF COUNTRIES, NOTE SCHOLARS GREY E. BURKHART AND SEYMOUR E. GOODMAN, PORNOGRAPHY IS "ALMOST ALWAYS FIRST MENTIONED" WHEN IT COMES TO WHAT THE INTERNET "MAY DO TO NATIONAL, CULTURAL AND RELIGIOUS VALUES." AMONG OTHER TOPICS RAISED WERE "PROSELYTIZING BY OTHER RELIGIONS AND THE AVAILABILITY OF UN-ISLAMIC INFORMATION (SUCH AS HOW TO COMMIT SUICIDE), THE POTENTIAL EFFECTS ON WOMEN'S ROLES IN SOCIETY, [AND] DILUTION OF LOCAL CULTURAL NORMS." THESE CONCERNS, THEY WRITE, SURFACED "IN THE PRESS AND IN OUR INTERVIEWS WITH GOVERNMENT, BUSINESS, ACADEMIC, RELIGIOUS AND PRIVATE INDIVIDUALS."⁴¹

SAUDI ARABIA HAS GONE FURTHEST IN DEFINING THE SCOPE OF WHAT KIND OF DATA IT WISHED TO KEEP OFF THE INTERNET: ITS COUNCIL OF MINISTERS ISSUED A DECREE REQUIRING SERVICE PROVIDERS TO REFRAIN FROM "CARRYING OUT ANY ACTIVITIES VIOLATING THE SOCIAL, CULTURAL, POLITICAL, MEDIA, ECONOMIC, AND RELIGIOUS VALUES OF THE KINGDOM OF SAUDI ARABIA."⁴²

U.A.E. OFFICIALS TOLD HUMAN RIGHTS WATCH THAT KEEPING OUT PORNOGRAPHY WAS THE ONLY OBJECTIVE OF THE U.A.E.'S INTERNET CENSORSHIP REGIME. OFFICIALS OF OTHER COUNTRIES AND CORPORATE REPRESENTATIVES OF ISPs IN THE REGION HAVE SPOKEN MORE GENERALLY OF PROTECTING CULTURAL VALUES. FOR EXAMPLE, A REPRESENTATIVE OF TELEYEMEN, YEMEN'S MONOPOLY ISP, TOLD HUMAN RIGHTS THAT THE TELEYEMEN WAS UNDER "A GENERAL REQUIREMENT" TO "LIMIT ACCESS TO INFORMATION WHICH IS CONSIDERED TO BE UNDESIRABLE IN TERMS OF CAUSING OFFENCE AGAINST SOCIAL, RELIGIOUS, OR CULTURAL STANDARDS." LIKE THE U.A.E. AND SAUDI ARABIA, YEMEN FILTERS WHAT USERS CAN ACCESS THROUGH THE USE OF A PROXY SERVER AND "CENSORWARE."⁴³ A PROXY SERVER IS A DEVICE THAT IS INTERPOSED

⁴¹ GREY E. BURKHART AND SEYMOUR E. GOODMAN, "THE INTERNET GAINS ACCEPTANCE IN THE PERSIAN GULF," *COMMUNICATIONS OF THE ACM*, MARCH 1999, VOL. 41 NO.3. THE ACM IS THE ASSOCIATION FOR COMPUTING MACHINERY.

⁴² QUOTED IN *AL-JAZIRA* NEWSPAPER, MAY 6, 1999, AS REPORTED IN FOREIGN BROADCAST INFORMATION SERVICE, NEAR EAST AND SOUTH ASIA (HEREAFTER FBIS), MAY 12, 1999.

⁴³ LETTER TO HUMAN RIGHTS WATCH FROM CHRISTOPHER D. LEATHER, TELEYEMEN DIVISIONAL MANAGER, AUGUST 9,

BETWEEN USERS AND THE INTERNET: IN RESPONSE TO USER REQUESTS AND ACCORDING TO THE CRITERIA IT IS PROGRAMMED TO FOLLOW, THE PROXY EXAMINES MATERIAL REQUESTED BY A USER AND EITHER DELIVERS IT OR BLOCKS ITS DELIVERY.

PRO-ACTIVE APPROACHES BY GOVERNMENTS

GOVERNMENTS HAVE RESPONDED TO THE ADVENT OF THE INTERNET PRO-actively as well as by CENSORSHIP AND REGULATION. EVERY MIDDLE EAST GOVERNMENT HAS LAUNCHED ONE OR MORE WEB SITES TO GET ITS VOICE HEARD amidst the din of ALTERNATIVE INFORMATION SOURCES in CYBERSPACE.⁴⁴ SAUDI ARABIA, BAHRAIN, EGYPT, IRAN, ISRAEL, KUWAIT, MOROCCO, OMAN, TUNISIA AND THE PALESTINIAN AUTHORITY ARE AMONG THOSE THAT WEBCAST STATE RADIO AND/OR TELEVISION.

SAUDI ARABIA HAS INVESTED HEAVILY IN GETTING ITS MESSAGE OUT, THROUGH AN INTERNET PRESENCE (SEE, FOR EXAMPLE, THE OFFICIAL SITE <www.saudi.net>) AND ALSO THROUGH OWNERSHIP BY PRO-GOVERNMENT SAUDIS OF INFLUENTIAL EUROPE-BASED ARAB NEWSPAPERS, MAGAZINES, AND BROADCAST MEDIA. ONE APPARENT IMPETUS HAS BEEN A WISH TO COUNTER SMALL LONDON-BASED SAUDI DISSIDENT GROUPS, SUCH AS THE COMMITTEE FOR THE DEFENSE OF LEGITIMATE RIGHTS (<www.ummah.org.uk/cdlr>) AND THE MOVEMENT FOR ISLAMIC REFORM IN ARABIA (<www.miraserve.com>), WHICH HAD ACHIEVED A HIGH PROFILE THROUGH ADROIT USE OF FAX MACHINES AND THE INTERNET.⁴⁵

THE GOVERNMENT OF TUNISIA MAINTAINS SEVERAL SITES CONTAINING OFFICIAL INFORMATION AND LINKS TO PRO-GOVERNMENT MEDIA (SEE, E.G., <www.tunisiaonline.com>). ITS PUBLIC RELATIONS EFFORTS

⁴⁴ DIRECTORIES OF GOVERNMENT SITES CAN BE FOUND AT <www.cksoft.com/govt> AND <www.gora.stm.it/politic>. A BRIEF OVERVIEW IS PROVIDED IN JONATHAN B. LINCOLN, "MIDDLE EAST GOVERNMENTS ON THE WORLD WIDE WEB," WNEP RESEARCH NOTES, NO. 6 (WASHINGTON, DC: WASHINGTON INSTITUTE FOR NEAR EAST POLICY, FEBRUARY 1999).

⁴⁵ THE STRONGEST MANIFESTATION OF OFFICIAL DISPLEASURE WITH THE DISSIDENT GROUPS CAME IN 1995, WHEN THE SAUDIS THREATENED GREAT BRITAIN WITH A CUTOFF OF DEFENSE CONTRACTS IF CDLR SPOKESMAN MUHAMMAD MAS'ARI WAS NOT SOMEHOW SILENCED. THE BRITISH GOVERNMENT ATTEMPTED TO DEPORT MAS'ARI BUT WAS THWARTED BY BRITAIN'S COURTS.

were aided by a pro-Tunisian businessman in Paris who launched a web site that had an appearance likely to fool viewers into thinking they had accessed an Amnesty International web site about Tunisia. The site, <www.amnesty-tunisia.org> offered only favorable information about Tunisia's human rights record and nothing related to the findings of Amnesty International.⁴⁶

Numerous articles in the regional press have urged a more active "Arab" presence on the Internet. An article in the official Damascus daily *Tishrin*, deploring the fact that web-based resources dealing with the Arab-Israeli conflict were dominated by materials of Israeli origin, called for "check[ing] all that is placed on the Internet on Syria and confront[ing] it by giving explanations or correcting distorted information."⁴⁷ The Syrian Arab News Agency launched a web site in 1998 (<www.sana.org>) to propagate official news and viewpoints at a time when local Internet access was unavailable to the Syrian public.

In a few countries, national and local governments are using the Internet to make it easier for citizens to consult official information and communicate with authorities. Several of Jordan's government ministries, as well as the General Intelligence Services (<www.nic.gov.jo/gid>), maintain their own sites and invite e-mail correspondence. Morocco (<www.mincom.gov.ma>), Egypt (via <www.mfa.gov.eg>, the Foreign Ministry site), and the Palestinian Authority (<www.pna.net>) have taken steps in this direction. However, few Arab governments have embarked on a systematic effort to put online information that would enhance informed political participation by their publics—materials such as legal and regulatory codes, draft legislation, official reports and statistics, transcripts of press conferences and parliamentary debates, court rulings, and economic data used to define budget allocations.

⁴⁶ The businessman denied that the use of "amnesty" in the web site address was intended to fool users. See Country Profiles, below.

⁴⁷ Husayn al-Ibrahim, "The Internet and Informatics [sic] in the Arab-Israeli Conflict," *Tishrin*, February 23, 1998, as reported in FBIS, March 1, 1998.

VI. CYBERCENSORSHIP: ITS VARIOUS FORMS

THE INTERNET OFFERS PROTEAN POSSIBILITIES FOR EVADING CONTROLS ON THE FLOW OF INFORMATION. IN COUNTRIES WHERE THERE IS NO LOCAL ISP, PERSONS CAN, FOR THE PRICE OF AN INTERNATIONAL CALL, DIAL SERVICE PROVIDERS IN OTHER COUNTRIES. IF A WEB SITE IS BLOCKED, ITS SPONSORS OR FANS CAN CHANGE ITS ADDRESS OR "MIRROR" THE SAME CONTENT AT OTHER WORLD WIDE WEB SITES. LOCAL USERS CAN VIEW WEB SITES THAT ARE BLOCKED BY ACCESSING THEM VIA FREE "ANTI-CENSORSHIP PROXY (ACP) SERVERS."⁴⁰ THEY CAN ALSO HAVE PERSONS WHO ENJOY ACCESS TO CONTENT THAT IS BLOCKED LOCALLY E-

⁴⁰ BRIAN RISTUCCIA, AN AMERICAN WHO SET UP A FREE, WEB-BASED ANTI-CENSORSHIP PROXY (ACP) SERVER, <WWW.SIRIS.ML.ORG>, EXPLAINED THAT HIS ACP WORKS BY CREATING AN ALTERNATE NAMESPACE FOR THE ENTIRE INTERNET. "THIS MEANS THAT EVERY SITE ON THE ENTIRE INTERNET IS MADE TO APPEAR AS IF IT IS A PAGE ON MY SERVER....THE ACP SERVER IS A VERY EFFECTIVE INTERNET CENSORSHIP REPAIR TOOL BECAUSE IT TAKES ONLY ONE UNBLOCKED SITE TO UNBLOCK THE ENTIRE INTERNET." HE WARNED, HOWEVER, THAT IF SURVEILLANCE IS BEING CONDUCTED OF INTERNET USERS, THEIR ACTIVITIES VIA THE ACP SERVER ARE NOT PROTECTED FROM MONITORING. HE

MAIL IT TO THEM AS ATTACHED FILES. WARY E-MAIL CORRESPONDENTS CAN FOIL SURVEILLANCE BY USING PSEUDONYMOUS E-MAIL ACCOUNTS OR ENCRYPTION, OR BY ROUTING MESSAGES THROUGH A WEB-BASED RE-MAILING SERVICE THAT "ANONYMIZES" THEM BY STRIPPING INFORMATION THAT IDENTIFIES THE SENDER.

BUT IF THE TRICKS AVAILABLE TO USERS ARE BOUNTIFUL, SO IS THE TECHNOLOGY ON THE OTHER SIDE OF THE CAT-AND-MOUSE GAME. GOVERNMENTS MAY NOT BE ABLE TO STOP, BUT THEY CAN CERTAINLY SLOW THE FLOW OF "OBJECTIONABLE" CONTENT AND THUS BUY TIME TO ADJUST TO AN ERA IN WHICH THEIR ABILITY TO BLOCK OR CROWD OUT INFORMATION IS DIMINISHED.

STATE'S CAN DENY THE PUBLIC LOCAL ACCESS TO THE INTERNET ALTOGETHER, AS IRAQ, LIBYA, SYRIA AND, UNTIL RECENTLY SAUDI ARABIA HAVE DONE. BUT NEITHER SYRIA NOR SAUDI ARABIA HAS GONE SO FAR AS TO PROHIBIT POSSESSION OF MODEMS OR CONNECTIONS TO FOREIGN INTERNET PROVIDERS. BOTH RIYADH AND DAMASCUS HAVE THUS TOLERATED A LIMITED AND GRADUALLY INCREASING AMOUNT OF INTERNET ACCESS RATHER THAN ADOPT THE DRACONIAN MEASURES REQUIRED TO PREVENT ACCESS TO FOREIGN ISPS, WHICH WOULD LIKELY ANTAGONIZE THE MEMBERS OF THE PUBLIC WEALTHY ENOUGH TO AFFORD IT.

SAID IN MARCH 1999 THAT THE LATEST VERSION OF HIS ACP "MAKES IT MORE DIFFICULT FOR PROXY ADMINISTRATORS TO SEE WHAT SITES A PERSON HAS VIEWED, BECAUSE EACH URL IS ASSIGNED A RANDOM TIME-EXPIRED TOKEN THAT ONLY THE PROXY SERVER KNOWS THE ACTUAL VALUE FOR."

THE OSIRIS ACP RECEIVED HEAVY TRAFFIC FROM USERS IN THE UNITED ARAB EMIRATES, AMONG OTHER COUNTRIES, RISTUCCIA SAID, BUT WAS BEING BLOCKED BY THE SAUDI AUTHORITIES. E-MAIL COMMUNICATION FROM BRIAN RISTUCCIA TO HUMAN RIGHTS WATCH, JANUARY 7, 1999 AND MARCH 11, 1999.

GOVERNMENTS THAT PRESENTLY ALLOW PUBLIC LOCAL ACCESS TO THE INTERNET HAVE ADOPTED A RANGE OF METHODS TO REGULATE THAT ACCESS. THE GLOBAL INTERNET LIBERTY CAMPAIGN DIVIDES THESE METHODS INTO FOUR CATEGORIES: INTERNET-SPECIFIC LAWS; APPLICATION OF EXISTING LAWS; CONTENT-BASED LICENSE (OR CONTRACT) TERMS APPLIED TO USERS AND SERVICE PROVIDERS, AND COMPULSORY USE OF FILTERING, RATING OR CONTENT LABELING TOOLS.⁴⁹ ALL OF THESE METHODS CAN BE FOUND IN THE MIDDLE EAST AND NORTH AFRICA, ALONG WITH EXTRA-LEGAL MEASURES THAT ALSO DIMINISH ONLINE FREEDOMS.

LAWS AND LICENSING TERMS. TUNISIA HAS DEVELOPED THE REGION'S MOST DETAILED INTERNET-SPECIFIC LAWS. TUNISIA ALSO EXPLICITLY EXTENDS TO THE INTERNET EXISTING PRESS LAWS LIMITING FREE EXPRESSION, SOMETHING THAT FEW OTHER COUNTRIES IN THE REGION HAVE DONE. HOWEVER, THE EXISTING PRESS LAWS OF SEVERAL COUNTRIES, IN THEIR DELINEATION OF OFFENSES, DEFINE "PUBLISHING" OR "DISSEMINATING" INFORMATION IN SO BROAD A FASHION THAT NO NEW LAWS ARE NEEDED TO BRING INTERNET SPEECH UNDER THEIR PURVIEW. QATARI INTERNET USERS MUST SIGN A CONTRACT WITH THE QATAR PUBLIC TELECOMMUNICATIONS CORPORATION (QTEL) PLEDGING NOT TO USE THE SERVICE TO "CARRY OUT ANY ACTIVITY WHICH IS CONTRARY TO PUBLIC ORDER" (ARTICLE 3.2.4). ASKED FOR THE DEFINITION OF THIS PHRASE, QATAR'S EMBASSY IN WASHINGTON REPLIED THAT WHILE THERE IS NO "CONCISE DEFINITE CONTEXT OF THE PHRASE," IT "REFERS IN GENERAL TO THE NECESSITY OF COMMITMENT TO THE STATE'S PUBLIC POLICIES AND TO THE COMMUNITY'S TRADITIONS AND VALUES."⁵⁰

FILTERING OF CONTENT. THE UNITED ARAB EMIRATES HAS SET UP A "PROXY SERVER" THAT DENIES USER ACCESS TO SITES DEEMED INAPPROPRIATE, MOSTLY BECAUSE OF THEIR EXPLICIT SEXUALITY. BAHRAIN, IRAN, YEMEN, TUNISIA, AND SAUDI ARABIA ALSO BLOCK WEB SITES, USING A VARIETY OF TECHNICAL MEANS AVAILABLE TO FILTER AND BLOCK CONTENT. BLOCKING IS EASIER TO IMPLEMENT FOR GOVERNMENTS THAT RETAIN CONTROL OVER THE NATIONAL TELECOMMUNICATIONS NETWORK, INCLUDING THE INTERNATIONAL GATEWAYS. NEARLY EVERYWHERE IN THE REGION, TELECOMMUNICATIONS REMAIN A STATE-CONTROLLED MONOPOLY. AND EVEN IN THE FEW COUNTRIES THAT HAVE ALLOWED SOME PRIVATIZATION OF INTERNET SERVICES, SUCH AS EGYPT, THE INTERNATIONAL GATEWAY REMAINS UNDER STATE CONTROL.

IN ADDITION TO TECHNICAL AND LEGAL MEANS, OTHER GOVERNMENT PRACTICES, INCLUDING THREATS AND INTIMIDATION, CAN CREATE A CHILLING EFFECT ON ONLINE SPEECH, JUST AS SUCH PRACTICES OFTEN DO MORE THAN PRESS LAWS TO CONSTRAIN WHAT PRIVATE NEWSPAPERS AND MAGAZINES ARE WILLING TO

⁴⁹ GLOBAL INTERNET LIBERTY CAMPAIGN, *REGARDLESS OF FRONTIERS*, PP. 11-12.

⁵⁰ UNDATED WRITTEN COMMUNICATION TO HUMAN RIGHTS WATCH, RECEIVED NOVEMBER 1998 AND REPRINTED IN APPENDIX C.

PRINT. FEARS OF GOVERNMENT SURVEILLANCE OR REPRISALS, FOR EXAMPLE, CAN FOSTER SELF-CENSORSHIP IN A NEWSPAPER, A WEB SITE, OR AN ONLINE "CHAT ROOM." IN JORDAN, FOR EXAMPLE, AT LEAST TWO PERSONS WERE REPORTEDLY SUMMONED FOR QUESTIONING BY THE POLICE DURING 1996 BECAUSE OF ARTICLES OR COMMENTS THEY HAD POSTED ON ELECTRONIC BULLETIN BOARDS OR IN CHAT ROOMS—FORUMS WHOSE CONTENTS CAN BE READ BY EVERYONE, INCLUDING THE POLICE (SEE SECTION ON JORDAN, BELOW).

NO GOVERNMENT IN THE REGION, TO OUR KNOWLEDGE, HAS ADMITTED TO "EAVESDROPPING" ON E-MAIL, AND HUMAN RIGHTS WATCH HAS NO PROOF THAT IT IS TAKING PLACE. YET GIVEN THE TECHNICAL EASE OF CONDUCTING THIS SORT OF SURVEILLANCE—ESPECIALLY WHEN ALL INTERNET ACCESS GOES THROUGH A GATEWAY THAT IS MAINTAINED BY A STATE-CONTROLLED INSTITUTION— AND THE FACT THAT POLICE FORCES IN SO MANY COUNTRIES OF THE REGION TAP THE PHONES AND OPEN THE MAIL OF REAL AND SUSPECTED DISSIDENTS, IT IS NOT SURPRISING TO HEAR FEARS EXPRESSED BY INTERNET USERS IN TUNISIA, SAUDI ARABIA, AND OTHER COUNTRIES ABOUT THE PRIVACY OF THEIR ELECTRONIC COMMUNICATIONS. AUTHORITIES MONITOR TELEPHONE CONVERSATIONS IN AT LEAST THIRTEEN COUNTRIES OF THE REGION, ACCORDING TO THE U.S. DEPARTMENT OF STATE'S *COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES* FOR 1999, AND IN MOST THEY DID SO WITHOUT LEGALLY ISSUED WARRANTS OR JUDICIAL SUPERVISION. THOSE WHO SUSPECT ONLINE SURVEILLANCE OFTEN CITE INSTANCES OF E-MAILS INEPLICABLY DISAPPEARING EN ROUTE OR TAKING TWO DAYS TO REACH THEIR DESTINATION. SUCH OCCURRENCES CAN BE CAUSED BY SNOOPING BUT OF COURSE MAY HAVE OTHER EXPLANATIONS AS WELL.

GOVERNMENTS HAVE ALSO PURSUED OLD-FASHIONED FORMS OF SURVEILLANCE AGAINST ONLINE EXPRESSION. IN MARCH 1997 SAUDI ARABIA'S AUTHORITIES DETAINED A TELECOMMUNICATIONS ENGINEER SUSPECTED OF TRANSMITTING INFORMATION TO OPPOSITION GROUPS ABROAD VIA HIS COMPUTER, WHICH WAS CONFISCATED. ACCORDING TO SOURCES ABROAD, THE ENGINEER, SAYYID 'ALAWI SAYYID SHARAF, CAME UNDER SUSPICION NOT THROUGH HIGH-TECH SURVEILLANCE BUT THROUGH THE TRADITIONAL METHODS OF THE SECRET POLICE, INCLUDING THE INTERROGATION OF THIRD PARTIES AND THE USE OF INFORMANTS (SEE SECTION ON SAUDI ARABIA, BELOW).

VII. GOVERNMENT-IMPOSED FILTERING SCHEMES VIOLATE THE RIGHT TO FREE EXPRESSION

GOVERNMENT-IMPOSED FILTERING POSES TWO BASIC THREATS TO THE RIGHT TO FREE EXPRESSION. FIRST, AS EXPLAINED IN THE LEGAL SECTION ABOVE, IT CONSTITUTES A FORM OF PRIOR CENSORSHIP AND AS SUCH SHOULD BE SUBJECTED TO THE STRICTEST LEVEL OF SCRUTINY. SECOND, IN PRACTICAL TERMS, THE FILTERING TECHNOLOGIES DEVELOPED SO FAR ARE IMPRECISE TOOLS. EVEN WHEN THE STATED MOTIVES FOR CONTENT-FILTERING HAVE BEEN JUSTIFIABLE, SUCH AS TO KEEP PORNOGRAPHIC MATERIALS FROM MINORS,⁵¹ THE MEANS USED HAVE ALMOST INVARIABLY IMPEDED, WHETHER INTENTIONALLY OR NOT, THE FLOW OF POLITICAL, CULTURAL, MEDICAL AND OTHER TYPES OF CONTENT THAT ARE UNQUESTIONABLY LEGAL UNDER INTERNATIONAL STANDARDS.

IN BAHRAIN, IRAN, SAUDI ARABIA, THE UNITED ARAB EMIRATES, AND YEMEN, ISPS—EITHER UNDER GOVERNMENT ORDERS OR PRESSURE—ALL BLOCK WEB SITES ON THE BASIS OF THEIR CONTENT.⁵² IN THE FIRST FOUR IF NOT ALL OF THESE COUNTRIES, BLOCKING EXTENDS TO CULTURAL AND/OR POLITICAL CONTENT.

U.A.E. OFFICIALS ARE PERHAPS MORE FORTHCOMING THAN OTHERS THAT ENGAGE IN BLOCKING. THEY JUSTIFY IT AS A MEANS OF LIMITING ACCESS TO PORNOGRAPHY. PERSONS IN THE EMIRATES WHO DIAL UP A LOCAL SERVICE PROVIDER DO NOT HAVE UNMEDIATED ACCESS TO THE INTERNET. RATHER, THEIR REQUESTS ARE ROUTED THROUGH A PROXY SERVER MAINTAINED BY THE GOVERNMENT-CONTROLLED TELECOMMUNICATIONS COMPANY, Etisalat.⁵³ WHEN A USER REQUESTS A WEB SITE, THE REQUEST WILL BE REFUSED IF THE

⁵¹ THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS PERMITS, IN ARTICLE 19, RESTRICTIONS ON SPEECH “FOR THE PROTECTION OF...PUBLIC HEALTH OR MORALS”—BUT ONLY “SUCH AS ARE PROVIDED BY LAW AND ARE NECESSARY.”

⁵² IT IS OFTEN DIFFICULT TO CONFIRM WHICH WEB SITES ARE BEING BLOCKED BY A GOVERNMENT AND FOR WHAT DURATION. THE INACCESSIBILITY OF A SITE MAY HAVE OTHER CAUSES SUCH AS A SURGE IN DEMAND OR TECHNICAL GLITCHES. ALSO, GOVERNMENTS GENERALLY DO NOT COMMENT ON WHICH WEB SITES THEY BLOCK, AND SITES SOMETIMES ARE BLOCKED ONLY INTERMITTENTLY.

⁵³ USERS CAN CIRCUMVENT THE U.A.E.’S PROXY SERVER IF THEY DIAL INTO AN ISP IN ANOTHER COUNTRY, OR IF

FILTERING SOFTWARE ON THE PROXY SERVER DETECTS "OBJECTIONABLE" MATERIAL ON THE SITE OR FINDS THAT THE SITE IS ON A LIST OF BANNED SITES. THE PRESENCE ON THE U.A.E.'S LIST OF TABOO SITES OF A POLITICAL AND CULTURAL WEB SITE FOR ARAB HOMOSEXUALS REFUTES OFFICIAL CLAIMS THAT ONLY PORNOGRAPHY IS BANNED (SEE BELOW).

THEY CAN ACCESS AN ANTI-CENSORSHIP PROXY SERVER.

A proxy server such as the ones in place in the U.A.E. and Saudi Arabia can be used by authorities to track which computer terminals are accessing which web sites and for how long. U.A.E. authorities deny monitoring individual web use. In Saudi Arabia, however, users who request a site that is blocked get a message on their screens warning that all access attempts are logged.⁵⁴

State-controlled or state-influenced Internet Service Providers in Tunisia, Iran, and Bahrain block web sites containing political or human rights criticism of the government. Tunisia has acknowledged blocking only those sites that offend moral values, but apparently this includes the sites of various human rights organizations critical of the government (see below).

Bahrain has been less aggressive than neighboring Saudi Arabia and the U.A.E. in trying to block pornography centrally. Although there are reports that it is blocking some sexually explicit sites, Batelco, the state-controlled monopoly service provider, seems to rely more on encouraging subscribers to download filtering programs, should they desire it.

The ability of minors to access online pornography was one impetus for the enactment in 1996 by the U.S. Congress of the Communications Decency Act (CDA). The act criminalized online communication that is "obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass another person," or "obscene or indecent" if the recipient of the communication is under eighteen years of age.

The CDA was opposed by a coalition of human rights and free expression groups. As Human Rights Watch, a member group of the coalition, argued in an affidavit to the Supreme Court, the law's prohibition of "indecent" speech could be applied to its own human rights reporting that includes graphic accounts of rape and other forms of sexual abuse. In an important ruling for Internet liberties, the U.S. Supreme Court in 1997 voided key provisions of the act on the grounds that the Internet is entitled to the highest level of free speech protection and the act violated that principle.⁵⁵

⁵⁴ Douglas Jehl, "The Internet's 'Open Sesame' Is Answered Warily," *New York Times*, March 19, 1999.

⁵⁵ *Reno v. American Civil Liberties Union*, 117 S. Ct. 2529, 138 L.Ed.2d. 974 (1997).

WHILE CAUTIONING THAT ALL METHODS OF CONTROLLING ACCESS TO INTERNET CONTENT POSE DANGERS TO THE RIGHT TO IMPART AND RECEIVE INFORMATION, SOME INTERNATIONAL CIVIL LIBERTIES ORGANIZATIONS HAVE ARGUED THAT FILTERING SOFTWARE INSTALLED BY THE END-USER RAISES FEWER FREEDOM-OF-SPEECH CONCERNS THAN CENSORSHIP IMPOSED FROM ABOVE.⁵⁶

FILTERING SOFTWARE WORKS BY EXAMINING A DATA STREAM AND BLOCKING ANY MATERIAL THAT MATCHES SPECIFIED CRITERIA, SUCH AS THE PRESENCE OF "STOP WORDS" IN A WEB SITE'S HOME PAGE OR URL, OR THE PRESENCE OF THE URL ON A LIST OF BANNED SITES. A MORE AGGRESSIVE TYPE OF SOFTWARE, SUCH AS THE KIDDESK INTERNET SAFE PROGRAM, "WHITE-LISTS" MATERIAL BY PROHIBITING ACCESS TO ALL MATERIALS EXCEPT THOSE THAT ARE EXPLICITLY APPROVED BY THE PARENT OR SUPERVISOR.

MAKING THE CASE THAT END-USER FILTERING SOFTWARE IS A "LESSER EVIL," THE CENTER FOR DEMOCRACY AND TECHNOLOGY, A WASHINGTON, D.C.-BASED ORGANIZATION, ARGUES:

BY PLACING CONTROL OVER CONTENT IN THE HANDS OF INDIVIDUAL PARENTS, AS OPPOSED TO BUREAUCRATS AND PROSECUTORS, POLICY MAKERS CAN ASSURE FULL RESPECT FOR OUR CONSTITUTIONAL PROTECTION OF FREEDOM OF EXPRESSION AND ENABLE THE INTERNET TO GROW FREE FROM UNNECESSARY AND INEFFECTIVE REGULATORY INTERFERENCE....A GREAT VARIETY OF BLOCKING AND FILTERING SOFTWARE EXISTS WHICH CAN SERVE THE DIVERSITY OF FAMILY VALUES OF AMERICAN COMMUNITIES, PROVIDING CHOICE TO FAMILIES ONLINE WITHOUT INFRINGING THE CONSTITUTIONAL FIRST AMENDMENT RIGHTS OF INTERNET USERS.⁵⁷

⁵⁶ FOR A BRIEF ACCOUNT OF THE PROS AND CONS OF VARIOUS METHODS OF REGULATING ACCESS BY MINORS TO SEXUALLY EXPLICIT MATERIAL ONLINE, SEE JOSEPH WESTFALL, "CYBERSMUT," *ISSUES IN ETHICS*, VOL. 9 (WINTER 1999), PP. 6-10; REPRINTED IN *BUSINESS AND SOCIETY REVIEW*, NO.102/103 (1999), PP. 89-94.

⁵⁷ "INTERNET FAMILY EMPOWERMENT WHITE PAPER: HOW FILTERING TOOLS ENABLE RESPONSIBLE PARENTS TO

PROTECT THEIR CHILDREN ONLINE," A WHITE PAPER PREPARED BY THE CENTER FOR DEMOCRACY AND TECHNOLOGY, JULY 16, 1997, <www.cdt.org/speech/summary.html>. THE AMERICAN CIVIL LIBERTIES UNION WRITES, "WHILE USER-BASED BLOCKING PROGRAMS PRESENT TROUBLING FREE SPEECH CONCERNS, WE STILL BELIEVE TODAY THAT THEY ARE FAR PREFERABLE TO ANY STATUTE THAT IMPOSES CRIMINAL PENALTIES ON ONLINE SPEECH. IN CONTRAST, MANY OF THE NEW RATINGS SCHEMES [SYSTEMS IN WHICH CONTENT IS RATED ACCORDING TO CERTAIN CRITERIA AND INAPPROPRIATE MATERIAL IS THEN BLOCKED] POSE FAR GREATER FREE SPEECH CONCERNS THAN DO USER-BASED SOFTWARE PROGRAMS." "FAHRENHEIT 451.2: IS CYBERSPACE BURNING? HOW RATING AND BLOCKING PROPOSALS MAY TORCH FREE SPEECH ON THE INTERNET," AMERICAN CIVIL LIBERTIES UNION, AUGUST 7, 1997, <www.aclu.org/issues/cyber/burning.html>. SEE ALSO, CYBER-RIGHTS AND CYBER-LIBERTIES (UK), "WHO WATCHES THE WATCHMEN: INTERNET CONTENT RATING SYSTEMS AND PRIVATISED CENSORSHIP," NOVEMBER 1997, <www.cyber-rights.org/watchmen.htm>.

WHETHER EMPLOYED BY END-USERS OR GOVERNMENT SERVERS, FILTERING SOFTWARE IS AN IMPRECISE TOOL THAT IN PRACTICE ALMOST ALWAYS BLOCKS MATERIALS BEYOND ITS STATED PURPOSE. THIS IS TRUE EVEN OF THE MORE SOPHISTICATED PRODUCTS THAT ARE REGULARLY UPDATED BY STAFF MEMBERS WHO CHECK WEB SITES FOR "SUITABILITY."⁵⁸ ACCORDING TO POPULAR ANECDOTES, SOFTWARE THAT HUNTED FOR SPECIFIED "STOP WORDS" ENDED UP BLOCKING SITES THAT MENTIONED THE ENGLISH COUNTY OF MIDDLESEX AND RECIPES FOR CHICKEN BREASTS. ONE POPULAR PROGRAM BLOCKED A WEB SITE CONTAINING INFORMATION ON AIDS PREVENTION. EVEN A PRO-FILTERING WEB SITE WAS ONCE BLOCKED BY SURF WATCH, A LEADING FILTERING PROGRAM, BECAUSE IT SHARED A COMMERCIAL SERVER WITH A PORNOGRAPHIC SITE.⁵⁹

⁵⁸ SEE ELECTRONIC PRIVACY INFORMATION CENTER, "FAULTY FILTERS: HOW CONTENT FILTERS BLOCK ACCESS TO KID-FRIENDLY INFORMATION ON THE INTERNET," DECEMBER 1997, <www2.epic.org/reports/filter-report.html>. A BIBLIOGRAPHY OF REPORTS AND ARTICLES CRITICAL OF FILTERING SOFTWARE IS POSTED ON THE WEB SITE OF THE INTERNET FREE EXPRESSION ALLIANCE, <www.ifea.net>. SEE ALSO THE "CENSORSHIP - ACADEMIC & EDUCATIONAL - LIBRARY FILTERING" ARCHIVE ON THE WEB SITE OF THE ELECTRONIC FREEDOM FOUNDATION (<www.eff.org>). THE LATTER CONTAINS "KIDS AND THE INTERNET: THE PROMISES AND THE PERILS," A DECEMBER 1999 PAPER BY MEMBER ORGANIZATIONS OF THE INTERNET FREE EXPRESSION ALLIANCE WHICH CRITIQUES FILTERING SOFTWARE AND DISCUSSES ALTERNATIVES.

⁵⁹ MATT RICHTEL, "TABLES TURN ON A FILTERING SITE AS IT IS TEMPORARILY BLOCKED," *NEW YORK TIMES*, MARCH 11, 1999.

VIII. CONTENT AND CARRIER: THE QUESTION OF LIABILITY

THE DEVELOPMENT OF THE INTERNET HAS SPURRED THE PROMULGATION OF NEW LAWS, AS WELL AS THE OFTEN-HASTY APPLICATION TO THE INTERNET OF EXISTING MEDIA LAWS. ONE CONTROVERSY THAT HAS FLARED IN SEVERAL COUNTRIES IS OVER APPORTIONING LIABILITY FOR OBJECTIONABLE CONTENT THAT APPEARS ONLINE.⁶⁰ IS AN INTERNET SERVICE PROVIDER THAT HOSTS A WEB SITE OR "CHAT ROOM" RESPONSIBLE FOR ITS CONTENT, OR IS THE ORIGINATOR OF THE OFFENDING CONTENT (FOR EXAMPLE, THE AUTHOR) SOLELY RESPONSIBLE? AND SHOULD A CYBERCAFÉ BE RESPONSIBLE FOR MESSAGES SENT BY CLIENTS FROM ITS PREMISES?

AS NOTED ABOVE, THE RIGHT TO FREE EXPRESSION IS BEST SERVED BY LAWS THAT FOCUS LIABILITY ON THE ORIGINATOR OF THE OFFENDING CONTENT, RATHER THAN ON ITS CONDUIT. BUT AT LEAST ONE COUNTRY IN THE REGION, TUNISIA, HAS PROMULGATED LAWS HOLDING ISPS LIABLE FOR CONTENT, INCLUDING STATUTES REQUIRING THE ISP DIRECTOR TO "MAINTAIN CONSTANT OVERSIGHT OF THE CONTENT OF THE ISP'S SERVERS TO INSURE THAT NO INFORMATION REMAINS ON THE SYSTEM THAT IS CONTRARY TO PUBLIC ORDER AND GOOD MORALS."

THE EUROPEAN COMMISSION, IN A 1996 REPORT, STATED, "INTERNET ACCESS PROVIDERS AND HOST SERVICE PROVIDERS PLAY A KEY ROLE IN GIVING USERS ACCESS TO INTERNET CONTENT. IT SHOULD NOT HOWEVER BE FORGOTTEN THAT THE PRIME RESPONSIBILITY FOR CONTENT LIES WITH AUTHORS AND CONTENT PROVIDERS." ISPS "SHOULD NOT BE TARGETED BY THE INDIVIDUAL GOVERNMENTS AND LAW ENFORCEMENT BODIES WHERE THE ISPS HAVE NO CONTROL OF THE INTERNET CONTENT."⁶¹ THIS APPROACH WAS ENDORSED BY THE EUROPEAN PARLIAMENT ON MAY 13, 1998 AND BY THE COUNCIL OF THE EUROPEAN UNION IN A "RECOMMENDATION" FORMALLY ADOPTED ON SEPTEMBER 24, 1998.⁶²

⁶⁰ SEE <[WWW.GILC.ORG/SPEECH/LIABILITY](http://www.gilc.org/speech/liability)> FOR INFORMATION ABOUT ISP LIABILITY JURISPRUDENCE IN SEVERAL WESTERN COUNTRIES.

⁶¹ <WWW2.ECHO.LU/LEGAL/EN/INTERNET/COMMUNIC.HTML>.

⁶² "COUNCIL RECOMMENDATION OF 24 SEPTEMBER 1998 ON THE DEVELOPMENT OF THE COMPETITIVENESS OF THE

EUROPEAN AUDIOVISUAL AND INFORMATION SERVICES INDUSTRY BY PROMOTING NATIONAL FRAMEWORKS AIMED AT ACHIEVING A COMPARABLE AND EFFECTIVE LEVEL OF PROTECTION OF MINORS AND HUMAN DIGNITY," <http://europa.eu.int/comm/dg10/avpolicy/new_srv/recom-intro_en.htm>. FOR MORE ON EUROPEAN UNION POLICY TOWARD THE INTERNET, SEE PENNY CAMPBELL AND EMMANUELLE MACHET, "EUROPEAN POLICY ON REGULATION OF CONTENT ON THE INTERNET," IN THE NATIONAL COUNCIL FOR CIVIL LIBERTIES, ED., *LIBERATING CYBERSPACE: CIVIL LIBERTIES, HUMAN RIGHTS AND THE INTERNET* (LONDON: PLUTO PRESS, 1999), PP. 140-150.

IN THE U.S., THE COMMUNICATIONS DECENCY ACT OF 1996 CLEARLY DISTINGUISHES, FOR THE PURPOSE OF ASSIGNING LIABILITY, THE CONTENT PROVIDER FROM THOSE WHO TRANSMIT THE CONTENT. THE CDA'S SECTION 230(c)(1), AMENDING THE COMMUNICATIONS ACT OF 1934, STATES, "[N]O PROVIDER OR USER OF AN INTERACTIVE COMPUTER SERVICE SHALL BE TREATED AS THE PUBLISHER OR SPEAKER OF ANY INFORMATION PROVIDED BY ANOTHER INFORMATION CONTENT PROVIDER." SEVERAL EUROPEAN COUNTRIES HAVE ADOPTED OR PROPOSED LEGISLATION LIMITING THE LIABILITY OF ACCESS PROVIDERS FOR CONTENT PROVIDED BY THIRD PARTIES.⁶³

CYBERCAFÉS ARE SHOPS WHERE PERSONS CAN WALK IN OFF THE STREET AND USE INTERNET-CONNECTED COMPUTERS FOR A FEE. AMONG THEIR PATRONS ARE PERSONS WHO HAVE NO OTHER MEANS OF ACCESSING THE INTERNET, AS WELL AS PERSONS WHO SEEK A MEASURE OF ANONYMITY OR PRIVACY THEY FEEL THEY DO NOT HAVE WHEN USING THEIR OWN COMPUTERS. THE FLUID NATURE OF THE CLIENTELE OF CYBERCAFÉS HAS AROUSED CONCERNS AMONG SOME GOVERNMENTS. IN VIETNAM, SECURITY OFFICIALS SHUT DOWN A CYBERCAFÉ AFTER EXPRESSING OBJECTIONS TO E-MAILS THAT WERE ALLEGEDLY SENT FROM IT.⁶⁴ IN SINGAPORE, WHICH HAS LEGISLATION REGULATING CONTENT ON THE INTERNET AND IMPOSING OVERSIGHT RESPONSIBILITY ON ISPs, AN ANONYMOUS COMMENT IN FEBRUARY 1996 SENT FROM A CYBERCAFÉ TO THE <SOC.CULTURE.SINGAPORE> NEWSGROUP IMMEDIATELY RESULTED IN AN APOLOGY FROM THE CAFÉ'S OWNERS AND A DISSOCIATION FROM THE CONTENT OF THE POSTING. APPARENTLY FEARING GOVERNMENT PRESSURES, SEVERAL SINGAPOREAN CYBERCAFÉS THEN REPORTEDLY RECONFIGURED THEIR EQUIPMENT SO

⁶³ FOR EXAMPLE, GERMANY'S INFORMATION AND COMMUNICATIONS SERVICES ACT, ARTICLE 1 SECTION 5, STATES, "[INTERNET SERVICE] PROVIDERS SHALL NOT BE RESPONSIBLE FOR ANY THIRD-PARTY CONTENT WHICH THEY MAKE AVAILABLE FOR USE UNLESS THEY HAVE KNOWLEDGE OF SUCH CONTENT AND ARE TECHNICALLY ABLE AND CAN REASONABLY BE EXPECTED TO BLOCK THE USE OF SUCH CONTENT." BUT THIS LEGISLATION DOES NOT FULLY ALLAY FREE-SPEECH CONCERNS ABOUT THE BURDEN PLACED ON THE ISP.

⁶⁴ DAVID CASE, "BIG BROTHER IS ALIVE AND WELL IN VIETNAM—AND HE REALLY HATES THE WEB," *Wired*, vol. 5, no.11 (November 1997).

that patrons could browse but no longer post material in newsgroups.⁶⁵ In Tunisia, at least some Internet cafés pursue practices that limit user privacy and anonymity, according to a European journalist who visited two locations in Greater Tunis in February 1999. The terminals in both shops were arranged so that all of the monitor screens were visible from a single point in the room. In one location, clients were required to present identity documents to the staff; in the other they were required to provide their names and addresses.

⁶⁵ Gary Rodan, "The Internet and Political Control in Singapore," *Political Science Quarterly*, vol. 113, no. 1, Spring 1998, pp. 63-90, <<http://efn.org/psq/rodan.html>> or <<http://tap.efn.org/psq/rodan.html>>.

IX. HOW USERS CAN PROTECT THEIR RIGHTS TO PRIVACY AND ANONYMITY

INTERNET COMMUNICATION IS HIGHLY VULNERABLE TO SURVEILLANCE AND INTERCEPTION. A GOVERNMENT AGENCY CAN VIOLATE THE PRIVACY OF E-MAIL CORRESPONDENCE JUST AS EASILY AS IT CAN TAP A PERSON'S TELEPHONE IN ORDER TO LISTEN TO CONVERSATIONS OR INTERCEPT FAXES. THE EQUIPMENT NEEDED IS NEITHER COSTLY NOR COMPLICATED TO OPERATE. AUTHORITIES CAN MONITOR BY TAPPING AN INDIVIDUAL PHONE LINE AND INTERCEPTING DATA STREAMS AS THEY ARE SENT AND RECEIVED. IF A USER HAS INTERNET ACCESS VIA A PRIVATE ISP, EMPLOYEES OF THAT ISP CAN OPEN AND READ E-MAIL SENT THROUGH IT OR ALLOW POLICE INVESTIGATORS TO DO SO, UNLESS SPECIAL SAFEGUARDS ARE PUT IN PLACE TO PROTECT PRIVACY. IF AUTHORITIES HAVE ACCESS TO AN ISP'S SERVER OR THE COUNTRY'S TELECOMMUNICATIONS NETWORK, THEY CAN CAPTURE E-MAILS WHILE THEY ARE IN TRANSIT.

AUTHORITIES CAN READ, BLOCK, OR DELETE MESSAGES BASED ON SUCH CRITERIA AS THE E-MAIL ADDRESS OF THE SENDER OR THE RECIPIENT, THE INTERNET PROTOCOL ADDRESSES IDENTIFYING THE SENDING COMPUTER AND THE DESTINATION COMPUTER(S), OR THE PRESENCE OF SPECIFIED CHARACTER STRINGS IN THE BODY OF THE MESSAGE—say, THE WORDS "EMIR" AND "CORRUPTION" IN CLOSE PROXIMITY. SUCH A SYSTEM IS ANALOGOUS TO A POSTAL DELIVERY SYSTEM IN WHICH ALL PIECES OF MAIL ARE FIRST DELIVERED TO A SINGLE LOCATION, WHERE OFFICIALS CAN INSPECT ITEMS AT WILL.

ALTHOUGH DATA IS BROKEN UP AND SENT IN "PACKETS," EACH PACKET CONTAINS INTERNET PROTOCOL (IP) ADDRESSES. PACKETS CAN EASILY BE REASSEMBLED WHILE EN ROUTE WITH THE AID OF EAVESDROPPING TOOLS.

AN EAVESDROPPER CAN GENERALLY IDENTIFY THE COMPUTER TERMINAL THAT IS SENDING OR RECEIVING DATA, BUT NOT THE PERSON WHO IS TYPING ON ITS KEYBOARD. FOR THIS REASON, SOME GOVERNMENTS ARE UNEASY ABOUT ALLOWING COMPUTER TERMINALS WITH INTERNET ACCESS IN PLACES WHERE EXTRA EFFORT WOULD BE REQUIRED TO MONITOR WHO IS USING EACH TERMINAL, FOR WHAT, AND WHEN. A CONTRACT PROVIDED BY TUNISIA'S STATE-RUN AGENCE TUNISIENNE D'INTERNET (ATI) REQUIRES INSTITUTIONAL INTERNET SUBSCRIBERS TO REFRAIN FROM OFFERING ANYONE REMOTE ACCESS VIA THEIR COMPUTERS WITHOUT PRIOR AUTHORIZATION, AND TO DECLARE TO THE ATI THE NAMES OF ALL PERSONS HAVING ACCOUNTS ON, OR ACCESS TO, THE COMPUTERS AND TO INFORM THE AGENCY OF CHANGES IN THE USER LIST.

EXPRESSION VIA THE INTERNET INCLUDES THE USE OF MEANS THAT ARE PRIVATE AND OTHERS THAT ARE PUBLIC. E-MAIL IS PRIVATE IN THE SENSE THAT THE SENDER SPECIFIES THE PERSONS AND ADDRESSES TO WHOM IT WILL BE SENT. (OF COURSE, RECIPIENTS CAN THEN RE-SEND IT TO OTHERS OR POST IT ON A BULLETIN BOARD, JUST AS THEY CAN DO WITH AN ORDINARY LETTER.) BY CONTRAST, LAUNCHING AN OPEN-ACCESS WEB SITE OR POSTING A COMMENT IN A PUBLIC NEWSGROUP ARE ACTS OF PUBLIC SPEECH SINCE THEY ARE VIEWABLE BY ANYONE WHO WISHES TO VISIT THE WEB SITE OR NEWSGROUP.

COMPUTER USERS HAVE VARIOUS MEANS TO PROTECT THEIR PRIVACY AND ANONYMITY, SOME MORE EFFECTIVE THAN OTHERS. AT THE LOW-TECH END, A USER CAN TRY TO AVOID SURVEILLANCE BY USING A COMPUTER TERMINAL OR E-MAIL ACCOUNT THAT IS NOT BEING MONITORED, FOR EXAMPLE, ONE BELONGING

to a friend. The user can dial into another country and bypass the local service provider or use a pseudonymous e-mail account from one of the many companies that offer web-based e-mail accounts and that do not require clients to furnish their real names, such as MSN.com's "Hotmail," Yahoo.com's "Yahoo! mail," and USA.net's "Web@ddress." These techniques may help users escape identification if they are not already under surveillance, but they are no insurance against interception if a user's computer communication is being monitored.⁶⁶

Experts agree that there are basically three methods that, for the time being at least, make surveillance extremely difficult: direct-to-satellite and other forms of wireless transmission, anonymous re-mailers, and encryption.

Small dishes are available that enable users to transmit and receive data directly via satellite, bypassing the ground-based telecommunication system. These fit into a suitcase-sized carrying case and can be placed discreetly on a balcony while in use. They resemble in size the "pizza" dishes used to download satellite television broadcasts, but are capable of sending as well as receiving. Some countries of the Middle East and North Africa either ban or require permits for direct-to-satellite dishes. Cost also puts this technology beyond the reach of most individuals and nongovernmental organizations in the region. But as they grow more affordable and widespread, wireless communications offer a potent means of evading government monitoring and censorship.

⁶⁶ Most web-based free e-mail services are not encrypted. Users could enhance security when using these services by encrypting and/or anonymizing the messages they send. See below.

Encryption, on the other hand, costs nothing or next to nothing. Strong and easy-to-use encryption software, such as the "Pretty Good Privacy" (PGP) program, can be downloaded for free from the World Wide Web and stored on a laptop or personal computer.⁶⁷ While experts using powerful computers have been able to break strong encryption codes, the process requires considerable resources and time and is impractical for routine monitoring. Users should nevertheless pay attention to developments in the field—as well as to local laws governing the use of encryption. The Global Internet Liberty Campaign maintains a country-by-country review of legislation at <www.gilc.org/crypto/crypto-survey.html#country>.

The right to encrypt messages is of particular importance to the protection of human rights. In many countries human rights organizations use PGP to protect the identity of witnesses and victims when sending data electronically. Rights groups in Guatemala, Ethiopia, Haiti, Mexico, South Africa, Hong Kong, and Turkey are among those that use encryption, according to the GILC survey. Some groups use cryptographic techniques to digitally sign messages that they send over the Internet to ensure their integrity and authenticity, that is, to prove the messages are indeed coming from them and have not been altered in transmission.

⁶⁷ See Patrick Ball and Mark Girouard, *Safe Communications in a Dangerous World: Cryptographic Applications for Human Rights Groups* (Washington, DC: American Association for the Advancement of Science, expected 1999). For information about how PGP, a "public key" encryption program, works, see the FAQ (Frequently Asked Questions) sheets at <<http://www.arcs.unm.edu/~drosOFF/pgp/pgp.html>> and <www.com.ac.uk/pgp.net/pgpnet/pgp-faq>; see also David Banisar, *Bug Off! A Primer for Human Rights Groups on Wiretapping* (London: Privacy International, October 1995), <www.privacy.org/pi/reports/bug_off.html>.

THE POWER OF ENCRYPTION TO FOIL MONITORING HAS LED A NUMBER OF GOVERNMENTS TO IMPOSE RESTRICTIONS ON THE USE, SALE, AND EXPORT OF ENCRYPTION SOFTWARE. TUNISIA, SAUDI ARABIA, AND ISRAEL ARE AMONG THOSE COUNTRIES THAT BAN THE USE OF ENCRYPTION WITHOUT PRIOR AUTHORIZATION.⁶⁶

ENCRYPTION HAS AN ACHILLES HEEL: IT MAY EFFECTIVELY SHIELD A MESSAGE'S CONTENTS FROM AN EAVESDROPPER BUT NOT THE FACT THAT SOMETHING HAS BEEN ENCODED. THIS ALONE MAY LEAD TO HARSH CONSEQUENCES IF THE AUTHORITIES WISH TO PUNISH THE SENDER OR RECIPIENT, OR COERCE THEM TO DISCLOSE THE MESSAGE'S CONTENTS OR THEIR "PRIVATE KEYS." UPON OBTAINING THE LATTER, AUTHORITIES COULD THEN READ EVERY MESSAGE ENCRYPTED WITH THE USER'S "PUBLIC KEY" OR USE THE COMPROMISED PRIVATE KEY TO IMPERSONATE THAT USER IN CORRESPONDING WITH OTHERS.

⁶⁶ ACCORDING TO GILC'S ENCRYPTION SURVEY, OTHER COUNTRIES WITH LAWS RESTRICTING ENCRYPTION INCLUDE BELARUS, SINGAPORE, RUSSIA, PAKISTAN, CHINA, AND UNTIL JANUARY 1999, FRANCE. IN THE UNITED STATES, ENCRYPTING IS NOT REGULATED, BUT LAWS BAR U.S. COMPANIES FROM FREELY EXPORTING STRONG ENCRYPTION SOFTWARE WITHOUT A LICENSE, ON THE GROUNDS THAT ENCRYPTION WILL BE USED BY TERRORISTS, DRUG TRAFFICKERS, AND ORGANIZED CRIME GROUPS TO CONCEAL THEIR DEEDS.

One way to circumvent this danger is to camouflage encrypted messages by using steganography. This type of program hides one form of data inside another—for example, text inside a graphic image or a video or audio clip—in such a way that makes it more likely to escape detection by interlopers. For example, a sensitive document proving that a police unit moonlighted as a death squad can be encrypted and embedded in a photograph of a soccer team, and then e-mailed to a person outside the country who has the means to extract the document. Steganography software can be downloaded for free from the World Wide Web.⁶⁹ However, some experts warn that sophisticated eavesdroppers can detect when a file has something steganographically hidden in it.

The third anti-surveillance strategy is to route communications via secure and trusted web-based re-mailing services that forward them to the designated recipient only after expunging the original address and other identifying data.⁷⁰ To reduce traceability further, users can select re-mailers that keep no records of the addresses from which they receive, and to which they send, data. They can also program messages to pass through more than one re-mailer; some re-mailers do this automatically. And if their browser supports strong encryption, they can choose a re-mailer that encrypts all messages as they are sent to that re-mailer, which then sends them on to the intended recipient in decrypted form. In the latter scenario, even if an eavesdropper is “sniffing” a person’s Internet activities, the eavesdropper can at most discern that the person is visiting a particular web site but not the content of the messages that the person is sending, the intended recipients, or whether the person has encrypted messages before sending them.

⁶⁹ For more on steganography, see <<http://members.iquest.net/~mrmil/stego.html>>.

⁷⁰ Useful information about anonymous re-mailers can be found in the Anonymous Re-mailer FAQ (Frequently Asked Questions) by André Bocard, <www.well.com/user/abocard/remailer.html>. See also <www.anonymizer.com>, which offers anonymizing re-mailer and web-browser services, a FAQ, and links to other sites that deal with privacy on the World Wide Web. For a list of active anonymizing re-mailers, see <www.cs.berkeley.edu/~raph/remailer-list.html>.

FOR OBVIOUS REASONS, SOME GOVERNMENTS SEE ANONYMIZING RE-MAILERS AS UNDESIRABLE AND HAVE BLOCKED THEM.⁷¹ THE GOVERNMENTS OF CHINA, SINGAPORE, AND THE UNITED ARAB EMIRATES BLOCK THE WEB SITE OF [WWW.ANONYMIZER.COM](http://www.anonymizer.com), ONE OF THE BEST-KNOWN SUCH SERVICES, ACCORDING TO LANCE COTTRELL, PRESIDENT OF ANONYMIZER.COM.⁷² ANOTHER POTENTIAL PROBLEM WITH ANONYMIZERS IS THAT THEY DO NOT GUARANTEE THAT THE USER'S IDENTITY WILL REMAIN UNKNOWN TO THE ANONYMIZING SERVICE ITSELF OR TO THE USER'S ISP. RESEARCHER ARE ADDRESSING THIS CONCERN. ONE TOOL THAT IS STILL IN PROTOTYPE FORM IS "CROWDS." IT WORKS BY COLLECTING WEB USERS INTO A GEOGRAPHICALLY DIVERSE GROUP THAT PERFORMS WEB TRANSACTIONS ON BEHALF OF ITS INDIVIDUAL MEMBERS IN A WAY THAT PREVENTS WEB SERVERS, OTHER "CROWD" MEMBERS, AND EAVESDROPPERS FROM IDENTIFYING THE SENDER OF A PARTICULAR COMMUNICATION.⁷³

⁷¹ ON CONCERNS IN THE LAW-ENFORCEMENT COMMUNITY ABOUT ANONYMITY ON THE INTERNET, SEE STEVE LOHR, "PRIVACY ON INTERNET POSES LEGAL PUZZLE," *NEW YORK TIMES*, APRIL 19, 1999.

⁷² LANCE COTTRELL, "COMMERCIAL ANONYMITY," PAPER PRESENTED AT THE COMPUTERS, FREEDOM AND PRIVACY CONFERENCE IN WASHINGTON, DC ON APRIL 6, 1999, <www.cfp99.org/program/papers/cottrell.htm>.

⁷³ "CROWDS" AND OTHER NEW TOOLS FOR PROTECTING PRIVACY ONLINE ARE DESCRIBED IN *COMMUNICATIONS OF THE ACM*, FEBRUARY 1999 (VOL. 42, NO. 2). THE ACM IS THE ASSOCIATION FOR COMPUTING MACHINERY.

Y. COUNTRY PROFILES

THIS SECTION PROFILES THE STATE OF ONLINE LIBERTIES IN EIGHT COUNTRIES OF THE MIDDLE EAST AND NORTH AFRICA. THE TYPE OF INFORMATION IT CONTAINS VARIES FROM COUNTRY TO COUNTRY, AND IS NOT COMPREHENSIVE. THE LENGTH OF EACH CHAPTER ENTRY IS NOT NECESSARILY INDICATIVE OF THE EXTENT OF INTERNET CONTROL OR REGULATION IN THAT COUNTRY.

Bahrain

THE INTERNET IS THE ARENA OF TWO CONFLICTING OBJECTIVES OF THE BAHRAINI GOVERNMENT: ITS BID TO BECOME "THE TELECOMMUNICATIONS HUB OF THE GULF"⁷⁴ AND ITS DETERMINATION TO SUPPRESS INFORMATION CRITICAL OF THE RULE OF THE AL KHALIFA FAMILY. AUTHORITIES HAVE ON THE ONE HAND PROMOTED THE INTERNET, MAKING ACCESS AVAILABLE SINCE 1995 AND EASY TO OBTAIN. NO AUTHORIZATION IS REQUIRED TO LAUNCH A WEB SITE. SEVERAL INTERNET CAFÉS SERVE THE PUBLIC. ON THE OTHER HAND, THE SECURITY SERVICES ARE AWARE THAT THE BAHRAINI OPPOSITION HAS SKILLFULLY USED THE INTERNET TO COLLECT AND DISSEMINATE INFORMATION. THEY HAVE BLOCKED WEB SITES AND REPORTEDLY EMPLOY TECHNICAL EXPERTS TO ASSIST IN CONDUCTING SURVEILLANCE OF INTERNET USE.

ACCORDING TO ONE BAHRAINI PROFESSOR WHO WAS INTERVIEWED IN FEBRUARY 1999 AND REQUESTED ANONYMITY, "THE SITUATION OF THE INTERNET IS GOOD, BETTER THAN THE OVERALL HUMAN RIGHTS SITUATION, BECAUSE THE GOVERNMENT UNDERSTANDS ITS IMPORTANCE FOR MAINTAINING A COMPETITIVE BUSINESS EDGE, ESPECIALLY IN A SERVICE ECONOMY." BAHRAIN'S CONSTITUTION GUARANTEES FREEDOM OF SPEECH, OF THE PRESS, PRINTING AND PUBLICATION, "IN ACCORDANCE WITH THE CONDITIONS AND PROCEDURE SPECIFIED BY THE LAW." IT ALSO GUARANTEES PRIVACY OF POSTAL, TELEGRAPHIC AND TELEPHONIC COMMUNICATIONS. ARTICLE 26 STATES, "NO COMMUNICATIONS SHALL BE CENSORED NOR THE CONTENTS THEREOF REVEALED EXCEPT IN CASES OF NECESSITY PRESCRIBED BY THE LAW AND IN ACCORDANCE WITH THE PROCEDURES AND GUARANTEES STATED THEREIN."

DESPITE THESE CONSTITUTIONAL PROVISIONS, AUTHORITIES EXERCISE SWEEPING CONTROL OVER ALL LOCAL MEDIA AND MAKE PUBLIC CRITICISM OF GOVERNMENT OFFICIALS AND POLICIES OFF-LIMITS. ACCORDING TO THE U.S. STATE DEPARTMENT'S *COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES* FOR 1999,

⁷⁴ SEE, FOR EXAMPLE, "BAHRAIN: THE POWERHOUSE OF THE GULF," AN EIGHT-PAGE ADVERTISING SUPPLEMENT IN THE DECEMBER 21, 1999 ISSUE OF *NEWSWEEK* MAGAZINE, U.S. EDITION.

"TELEPHONE CALLS AND CORRESPONDENCE ARE SUBJECT TO MONITORING. POLICE INFORMER NETWORKS ARE EXTENSIVE AND SOPHISTICATED. DURING THE YEAR, THE GOVERNMENT FREQUENTLY INFRINGED ON CITIZENS' RIGHT TO PRIVACY, USING ILLEGAL SEARCHES AND ARBITRARY ARRESTS AS TACTICS TO CONTROL POLITICAL UNREST....E-MAIL ACCESS TO INFORMATION IS UNIMPEDED, ALTHOUGH IT MAY BE SUBJECT TO MONITORING."

BAHRAINI AUTHORITIES DID NOT RESPOND TO HUMAN RIGHTS WATCH'S LETTER AND FOLLOW-UP INQUIRIES REQUESTING INFORMATION ON INTERNET POLICIES. INTERNET SERVICE IS A MONOPOLY OF THE PUBLIC TELECOMMUNICATIONS COMPANY BATELCO. PRICES ARE MODERATE BUT CAN ADD UP SINCE THERE IS NO OPTION FOR UNLIMITED SERVICE AT A FIXED PRICE.

THERE ARE CONFLICTING REPORTS ON THE EXTENT TO WHICH AUTHORITIES BLOCK POLITICALLY SENSITIVE WEB SITES. HOWEVER, VARIOUS SOURCES CONCUR THAT THE WEB SITE OF THE BAHRAINI FREEDOM MOVEMENT (<http://ourworld.compuserve.com/homepages/bahrain>)—OR AT LEAST THE CONTENT BEYOND ITS HOME PAGE—is SYSTEMATICALLY BLOCKED. UNLIKE THE UNITED ARAB EMIRATES AND SAUDI ARABIA, BAHRAIN DOES NOT APPEAR TO HAVE IMPLEMENTED AN AMBITIOUS SYSTEM TO BLOCK PORNOGRAPHY. IT HAS PREFERRED TO ENCOURAGE USERS CONCERNED ABOUT SEXUALLY EXPLICIT MATERIALS TO INSTALL FILTERING SOFTWARE.

AUTHORITIES ARE LESS CONCERNED WITH BLOCKING WEB SITES THAN WITH CLOSING DOWN THE SOURCES OF CRITICAL INFORMATION LEAKING OUT OF THE COUNTRY, ACCORDING TO THE PROFESSOR CITED ABOVE. A SMALL NUMBER OF BAHRAINIS HAVE REPORTEDLY BEEN DETAINED OR QUESTIONED ON SUSPICION OF USING ELECTRONIC MEANS TO TRANSMIT INFORMATION TO POLITICAL OPPOSITION GROUPS OUTSIDE THE COUNTRY. THE BEST KNOWN CASE IS THAT OF SAYYID 'ALAWI SAYYID SHARAF, A BATELCO ENGINEER. ON THE NIGHT OF MARCH 25, 1997 SECURITY FORCES RAIDED SHARAF'S HOME, CONFISCATED HIS COMPUTER AND DETAINED HIM. HE WAS HELD FOR NEARLY TWO YEARS BEFORE BEING RELEASED WITHOUT CHARGE. ACCORDING TO A BAHRAINI WHO MET SHARAF AFTER HIS RELEASE, HE CAME UNDER SUSPICION NOT THROUGH HIGH-TECH MEANS OF SURVEILLANCE BUT THROUGH THE TRADITIONAL POLICE METHODS, INCLUDING THE INTERROGATION OF THIRD PARTIES AND THE USE OF INFORMANTS. AMNESTY INTERNATIONAL STATED THAT SHARAF HAD REPORTEDLY BEEN TORTURED WHILE BEING HELD INCOMMUNICADO BY INTELLIGENCE OFFICIALS.⁷⁵

IRAQ

⁷⁵ AMNESTY INTERNATIONAL URGENT ACTION APPEAL 42/97, MARCH 25, 1997.

Iraq is the only country in West Asia that has no Internet connection at all. In a letter to Human Rights Watch, Iraq's Ambassador to the United Nations Nizar Hamdoon blamed this state of affairs on damage to the telecommunications infrastructure inflicted during the Gulf War and to the U.N. sanctions⁷⁶ that restrict imports of spare parts for this sector. He suggested that but for these foreign obstacles, the government of Iraq would be pursuing a pro-Internet policy. In his letter, the ambassador affirmed that Iraq's constitutional guarantees of freedom of opinion encompass the right to receive and disseminate information online, "in conformity with the aims of the constitution and within the limits of the law." He added that the state "shall endeavor to provide the facilities needed for the exercise of this freedom."⁷⁷

⁷⁶ In response to Iraq's invasion of Kuwait in 1990, the Security Council prohibited all Iraqi exports and all imports except essential humanitarian items. U.N.S.C. resolution 697 (1991) conditioned the lifting of this embargo on a determination by the Security Council that the Iraqi government had complied with demands made in the resolution, including the destruction of its weapons of mass destruction and payment of reparations to Kuwait. Since 1995, the Security Council has allowed Iraq to export oil and use the proceeds to purchase humanitarian supplies, the selection and distribution of which is under U.N. supervision.

⁷⁷ Letter to Human Rights Watch from Nizar Hamdoon, the Permanent Representative of Iraq to the United Nations, June 1, 1999.

HOWEVER, GIVEN IRAQ'S INTOLERANCE OF ANY KIND OF POLITICAL DISSENT OR CRITICISM, IT IS HARDLY SURPRISING THAT IT REPORTEDLY PROHIBITS UNAUTHORIZED USE OF MODEMS, WHICH ARE A PREREQUISITE FOR GOING ONLINE.⁷⁹

⁷⁹ JOSH FRIEDMAN, A REPORTER FOR THE LONG ISLAND, NEW YORK-BASED *NEWSDAY*, TOLD HUMAN RIGHTS WATCH THAT WHEN HE AND TWO OTHER FOREIGN JOURNALISTS ENTERED IRAQ BY LAND FROM JORDAN IN DECEMBER 1999, IRAQI CUSTOMS AGENTS ASKED EACH ONE IF HE WAS CARRYING MODEMS OR SATELLITE PHONES. THEY DENIED HAVING MODEMS. THEY WERE OBLIGED TO PAY A FEE OF U.S. \$300 FOR EACH SATELLITE PHONE, WHICH THE AGENTS THEN SEALED WITH COPPER WIRE OSTENSIBLY TO PREVENT THEIR USE EXCEPT INSIDE THE PRESS CENTER OF THE MINISTRY OF COMMUNICATIONS IN BAGHDAD. TELEPHONE INTERVIEW, JANUARY 11, 1999.

THE OFFICIAL PRESS HAS BEEN OF TWO MINDS ABOUT THE INTERNET, DENOUNCING IT AS "ONE OF THE AMERICAN MEANS TO ENTER EVERY HOUSE IN THE WORLD" WHILE COVERING IT FAVORABLY ELSEWHERE.⁷⁹ IRAQI AUTHORITIES HAVE MOUNTED WEB SITES TO DISSEMINATE OFFICIAL INFORMATION. IN APRIL 1999 THE IRAQI NEWS AGENCY (INA) LAUNCHED AN ARABIC AND ENGLISH SITE, <www.nisciraq.net/iraqnews>. THE FOLLOWING MONTH, *al-Zawra* BECAME THE FIRST IRAQI NEWSPAPER TO LAUNCH AN ONLINE EDITION, HOSTING IT ON A WEB SITE BASED IN JORDAN, <www.indey.com.jo/iraqtoday/index.html>. IRAQ'S MISSION TO THE UNITED NATIONS HAS LONG HAD A SITE OF ITS OWN, <www.undp.org/missions/iraq/>.

DESPITE THE DAMAGE INFLICTED ON THE COUNTRY'S INFRASTRUCTURE DURING THE GULF WAR AND THE ENSUING SANCTIONS, THE GOVERNMENT OF IRAQ COULD SET UP SOME SORT OF INTERNET LINK FOR ITS CITIZENS IF IT HAD THE WILL TO DO SO, ACCORDING TO TELECOMMUNICATIONS EXPERTS. IN SULAYMANIYEH, A NORTHERN CITY THAT IS CONTROLLED BY A KURDISH FACTION, BEYOND THE REACH OF PRESIDENT SADDAM HUSSEIN'S SECURITY FORCES, INTERNET ACCESS HAS BEEN ESTABLISHED USING A SMALL SATELLITE DISH. THE LOCAL UNIVERSITY CONNECTS TO THE INTERNET VIA THAT LINK.⁸⁰

THE SANCTIONS REGIME HAS CONTRIBUTED TO A DRASTIC DROP IN IRAQ'S STANDARD OF LIVING, HEALTH CARE, AND EDUCATION AND SET BACK ITS TECHNOLOGICAL ADVANCEMENT. FOR MANY ORDINARY IRAQIS, THE HARDSHIPS OF DAILY SURVIVAL HAVE NO DOUBT MADE INTERNET ACCESS SEEM A REMOTE LUXURY. IN ADDITION, THE U.N. SANCTIONS REGIME HAS RESTRICTED THE IMPORT OF COMPUTERS AND PERIPHERALS, ALTHOUGH THE SECURITY COUNCIL'S SANCTIONS COMMITTEE HAS APPROVED SOME PURCHASES OF COMPUTERS FOR SCHOOLS, AND COMPUTER EQUIPMENT IS SMUGGLED INTO THE COUNTRY AND SOLD OPENLY.⁸¹

⁷⁹ FOR EXAMPLES OF IRAQI PRESS COMMENTARY ON THE INTERNET, SEE THE MOSAIC GROUP, *THE GLOBAL DIFFUSION OF THE INTERNET PROJECT: AN INITIAL INDUCTIVE STUDY*, MARCH 1999, PP. 102-103, <www.ogsd.com/gdi97/gdi97.html>.

⁸⁰ TELEPHONE INTERVIEW WITH BARIHAM SALEH, WASHINGTON REPRESENTATIVE OF THE PATRIOTIC UNION OF KURDISTAN PARTY, FEBRUARY 23, 1999.

⁸¹ SEE POLLY SPRENGER, "LEAST CONNECTED NATION STATUS," *WIRED NEWS ONLINE*, DECEMBER 17, 1999,

THE LACK OF INTERNET ACCESS IS MOST REGRETTABLE AT A TIME WHEN IRAQIS FEEL MORE CUT OFF THAN EVER FROM THE OUTSIDE WORLD. THE ISOLATION AND INTELLECTUAL DEPRIVATION WOULD NO DOUBT BE MITIGATED IF IRAQIS HAD GIVEN THE OPPORTUNITY TO COMMUNICATE INEXPENSIVELY VIA E-MAIL AND OBTAIN FROM THE WORLD WIDE WEB AND OTHER ONLINE SOURCES MATERIALS AND INFORMATION THAT IS ABSENT IN THEIR LIBRARIES AND NEWSSTANDS.

IRAQ'S OPPOSITION MOVEMENTS AND PARTIES IN EXILE, AS WELL AS THE KURDISH POLITICAL PARTIES THAT OPERATE IN THE NORTH OF THE COUNTRY BEYOND BAGHDAD'S CONTROL, MAINTAIN WEB SITES. IN ADDITION, MEMBERS OF THE IRAQI DIASPORA HAVE CREATED A CULTURAL WEB SITE, <www.iraq.net>, THAT BILLS ITSELF AS "A SMALL EFFORT TOWARDS BRINGING IRAQIS SCATTERED AROUND THE GLOBE, TO ONE PLACE, TO SHARE IDEAS, DISCUSS IRAQI CONCERNS, MEET OLD FRIENDS, MAKE NEW ONES OR SIMPLY...JUST TO HANG OUT!"⁹²

Jordan

INTERNET USE HAS GROWN RAPIDLY IN JORDAN, WITH THE GOVERNMENT EXTOLLING ITS VIRTUES AND IMPOSING FEW RESTRICTIONS. AUTHORITIES HAVE BEEN MORE TOLERANT TOWARD NEWS AND COMMENT ONLINE THAN TOWARD TRADITIONAL PRINT AND BROADCAST NEWS MEDIA, WITH THE RESULT THAT JORDANIANS CAN OBTAIN INFORMATION FROM THE INTERNET THAT IS EITHER TABOO OR IGNORED IN THE LOCAL PRINT PRESS.

INDIVIDUALS, CORPORATIONS, AND ORGANIZATIONS CAN ESTABLISH INTERNET ACCOUNTS EASILY. NO FORM OF GOVERNMENT APPROVAL OR REGISTRATION IS REQUIRED TO OPEN AN ACCOUNT OR SET UP A WEB SITE. HOWEVER, HIGH PHONE AND INTERNET ACCESS COSTS, INCLUDING TAXES AND FEES COLLECTED FROM ISPs, HAVE KEPT THE NUMBER OF USERS—ESTIMATED AT BETWEEN 20,000 AND 30,000—LOWER THAN IT MIGHT OTHERWISE BE. IN EARLY 1999, A MONTHLY ACCOUNT FOR A MODERATE USER COST THE EQUIVALENT OF U.S. \$70, INCLUDING PHONE CHARGES. ALTHOUGH THERE ARE SIX PRIVATE ISPs, ALL MUST GET THEIR LINES FROM THE STATE TELECOMMUNICATIONS COMPANY AND ARE CAPTIVE TO ITS RELATIVELY HIGH PRICING POLICIES.

<www.wired.com/news/news/politics/story/16904.html>, and JOSH FRIEDMAN, "THE BAGHDAD MARKETPLACE: DESPITE EMBARGO, SMUGGLERS KEEP RICH IRAQIS SUPPLIED," *NEWSDAY*, JANUARY 4, 1999, P. A14.

⁹² LISA NAPOLI, "IRAQI EXILES REACH FOR HOME ON WEB SITE," *NEW YORK TIMES*, FEBRUARY 20, 1997.

According to the government, "There is no blocking or censoring by the government of the content of any web sites or of electronic communications via newsgroups, e-mail or other Internet forums."⁹³ Human Rights Watch has heard no reports that contradict this assertion.

Privately run Internet cafés have proliferated in Amman and sprouted up in other cities.⁹⁴ The government states, "There are no special laws relating to their operation other than the standard licenses they have to obtain as any other business."⁹⁵ We are not aware of any form of government effort to restrict or monitor use of the Internet at cybercafés.

⁹³ Letter to Human Rights Watch from Marwan Muasher, Ambassador to the United States, May 21, 1999.

⁹⁴ A newspaper profile of cybercafés in Jordan reported that there were fourteen in Amman. Bassam Badareen, "Maqahi al-Internet fi Amman: al-Baith 'an at-Zawja al-Munasaba...wa Afdhal at-Turuk li-Suna' al-Qunbala an-Nuwayya," ("Cybercafés in Amman: Looking for a suitable wife...and the best way to build a nuclear weapon") *al-Quds al-Arabi*, September 29, 1999. An article in the October 6, 1999 *al-Sharq al-Awsat* reported that there were fifteen cybercafés in Amman and nearly twenty elsewhere in Jordan. As reported in FBIS, October 29, 1999.

⁹⁵ Letter from Ambassador Muasher.

THE JORDANIAN PUBLIC HAS BEEN ABLE TO OBTAIN INTERNET ACCESS LOCALLY SINCE 1996. THE LOCAL PROVIDERS OFFER NATIONAL ONLINE NEWSGROUPS (ELECTRONIC BULLETIN BOARDS) AND CHAT ROOMS.⁶⁶ IN THESE FORUMS, JORDANIANS HAVE BEEN ABLE TO CONVERSE ABOUT TOPICS THAT THE LOCAL PRESS HAS COVERED GINGERLY IF AT ALL, SUCH AS THE VIEWS AND IMPRISONMENT OF OUTSPOKEN POLITICAL DISSIDENT LEITH SHBEILAT (WHO HIMSELF HAS PARTICIPATED IN ONLINE DISCUSSIONS), "HONOR" KILLINGS, JORDAN'S CONTROVERSIAL PEACE TREATY AND RELATIONS WITH ISRAEL, AND ARMED ATTACKS ON ISRAELI TARGETS.

VARIOUS GOVERNMENT MINISTRIES HAVE WEB SITES AND E-MAIL ADDRESSES, INCLUDING THE GENERAL INTELLIGENCE DEPARTMENT (<www.nic.gov.jo/gid>). AT LEAST ONE INTERNET SERVICE PROVIDER, NETS, INVITES SUBSCRIBERS TO POST COMMENTS AND QUESTIONS TO PARTICIPATING GOVERNMENT OFFICIALS IN AN "ASK THE GOVERNMENT" FOLDER.

JORDANIANS HAVE BEEN ABLE TO GO ONLINE TO CIRCUMVENT OCCASIONAL PROHIBITIONS OF FOREIGN NEWSPAPERS. ON MAY 19, 1999, AUTHORITIES BANNED THE LONDON-BASED DAILY *AL-QUDS AL-ARABI* INDEFINITELY FROM IMPORTATION. ACCORDING TO EDITOR-IN-CHIEF ABDEL-BARRI ATWAN, OFFICIALS ACCUSED THE PAPER OF PUBLISHING STORIES HOSTILE TO JORDAN, BUT DID NOT SPECIFY WHICH.⁶⁷ IN THEIR MAY 23 ISSUES, VARIOUS JORDANIAN DAILIES AND WEEKLIES RAN ADVERTISEMENTS FROM *AL-QUDS AL-ARABI* REMINDING READERS THAT THE FULL TEXT OF THE NEWSPAPER WAS AVAILABLE DAILY AT <www.alquds.co.uk>. ACCORDING TO EDITOR ATWAN, THERE WERE NO REPORTS OF THE SITE BEING BLOCKED, AND MANY JORDANIANS READ THE NEWSPAPER ONLINE. *AL-QUDS* WAS LATER PERMITTED TO RESUME DISTRIBUTION OF ITS PRINT COPIES IN JORDAN.

⁶⁶ JED WEINER, "JORDAN AND THE INTERNET: DEMOCRACY ONLINE?" *MIDDLE EAST INSIGHT*, MAY-JUNE 1999, PP. 49-50.

⁶⁷ TELEPHONE INTERVIEW WITH HUMAN RIGHTS WATCH, MAY 26, 1999.

DESPITE A RELATIVELY UNFETTERED INTERNET, THE INCREASING RESTRICTIONS ON FREEDOM OF EXPRESSION AND THE PRESS IN JORDAN⁸⁸ HAVE CAST A SHADOW OVER INTERNET USE. IT IS WIDELY BELIEVED THAT JORDANIAN SECURITY AUTHORITIES READ THE COMMENTS POSTED IN THE CHAT ROOMS AND BULLETIN BOARDS ESTABLISHED BY JORDANIAN ISPs AS FORUMS ON DOMESTIC ISSUES. DURING 1996 THE INTELLIGENCE SERVICES SUMMONED AT LEAST TWO PERSONS FOR QUESTIONING OVER MESSAGES WITH POLITICAL CONTENT THAT THEY POSTED ON BULLETIN BOARDS OR CHAT GROUPS, ACCORDING TO THAMER A. OBEIDAT, AN OPPOSITION POLITICAL FIGURE. TWO JORDANIAN JOURNALISTS SEPARATELY CONFIRMED HIS ACCOUNT TO HUMAN RIGHTS WATCH. OBEIDAT SAID THE INDIVIDUALS DID NOT WANT THEIR IDENTITIES DISCLOSED FOR FEAR OF REPRISALS.⁸⁹

HUMAN RIGHTS WATCH IS UNAWARE OF SUCH INCIDENTS RECURRING AFTER 1996. HOWEVER, SEVERAL JORDANIAN INTERNET USERS TOLD HUMAN RIGHTS WATCH THAT WHILE DISCUSSIONS ABOUT DOMESTIC POLITICAL ISSUES IN THE CHAT ROOMS AND BULLETIN BOARDS ARE MORE WIDE-RANGING THAN THE LOCAL PRINT OR BROADCAST MEDIA, USERS FEARED REPERCUSSIONS IF THEY BROKE UNSPECIFIED RULES GOVERNING THE WAY ISSUES COULD BE DISCUSSED. MARWAN JOMA, THE GENERAL MANAGER OF NETS, ONE OF THE LARGEST PRIVATE ISPs, EXPLAINED IN A MAY 26, 1998 PHONE CONVERSATION WITH HUMAN RIGHTS WATCH:

THERE ARE VERY FEW RULES, BUT NETS, BEING IN JORDAN, HAS TO COMPLY WITH LOCAL LAWS. THIS MEANS USERS MUST NOT USE FOUL LANGUAGE NOR ATTACK PUBLIC FIGURES. YOU CAN ATTACK THE POLICY OF A CERTAIN MINISTER, BUT YOU CAN'T ATTACK [THEM OR OTHER] SUBSCRIBERS PERSONALLY. NETS DOESN'T SCREEN [I.E., CENSOR] MESSAGES, BUT WE READ THE MESSAGES, LIKE ANY OTHER USER, AND IF THERE'S A [TRANSGRESSION] WE SEND THE USER A REMINDER, AND WE CAN SUSPEND THEM FROM A [FORUM].

⁸⁸ SEE SA'EDA KILANI, *BLACK YEAR FOR DEMOCRACY IN JORDAN: THE 1998 PRESS AND PUBLICATION LAW* (COPENHAGEN: EURO-MEDITERRANEAN HUMAN RIGHTS NETWORK, SEPTEMBER 1998); HUMAN RIGHTS WATCH, "JORDAN: CLAMPING DOWN ON CRITICS: HUMAN RIGHTS VIOLATIONS," *A HUMAN RIGHTS WATCH REPORT*, VOL. 9, NO. 12, OCTOBER 1997; HUMAN RIGHTS WATCH, "JORDAN: A DEATH KNEEL FOR FREE EXPRESSION?" *A HUMAN RIGHTS WATCH REPORT*, VOL. 9, NO. 5, JUNE 1997.

⁸⁹ LETTER TO HUMAN RIGHTS WATCH, MAY 17, 1998.

Authorities directly pressured one online publication, Amin (Arab Media Internet Network, <www.amin.org>), which seeks to make available news and commentary not provided by the traditional media. Amin's Jordan office was opened in 1997 as a project of the nonprofit international organization Internews (<www.internews.org>), which supports independent media in what it describes as "emerging democracies" and works to combat censorship. Amin quickly attracted some of the country's most talented journalists as contributors. In addition to providing links to the web sites of over one hundred Arab newspapers, magazines, radio, and television stations, Amin posts on its "Eye on Amman" link the latest communiqués from human rights organizations and coverage of Jordan's parliament, nongovernmental organizations, and women's issues.

According to Ra'ed al-Abed, then managing editor at Amin, the advent of the service provoked the ire of certain government officials. While some of Jordan's print publications have Internet editions, Amin was the first local media organ that is based online. During the first half of 1999, Bilal al-Tal, then-director of the government's Office of Press and Publications, phoned Amin's offices on numerous occasions, warning the staff that they were not allowed to write about a particular topic, and that they were violating Jordanian law by operating without a license. However, al-Tal never formally initiated procedures to close down the agency. According to Fadi al-Qadi, the project director of Amin in Jordan, the agency applied for legal status as a nongovernmental organization in 1997, and in August 1999 that approval was granted.

A Jordanian journalist who is a fan of Amin commented to Human Rights Watch, "because the laws are not clear, Amin presents a new challenge: it's like a newspaper but the [authorities] cannot treat it as a publication. Yet when they saw the content, they didn't like it and so they started calling them and telling them they were violating the press law."

According to a former editor at Amin, the agency's web site pushed the limits of what was appearing in Jordan's other news media, but did not feature any item that officials had explicitly ordered newspapers not to publish. He observed, "We have to be careful because operating in Jordan...we can't talk freely about the royal family, we wouldn't think about it as long as the laws are what they are. These are 'red lines.' If it comes to analysis, that's okay, but you cannot point fingers at any of the royal family."⁹⁰

On September 1, 1999 the draconian Press and Publication Law took effect, restricting press freedom in a variety of ways. The broad language of this new legislation has been criticized by journalists and human rights activists in Jordan and overseas. Article 2, which defines "publication" as "any media in which meanings, words, or ideas are expressed in any way," could easily be interpreted to apply to online publications, although authorities have not to our knowledge explicitly stated this to be the case. Features of the new law that restrict free expression include requirements that:

⁹⁰ Telephone interview with Human Rights Watch, May 14, 1999.

- PRIVATE NON-DAILY PUBLICATIONS SECURE A MINIMUM CAPITAL OF 100,000 JORDANIAN DINARS (ABOUT U.S.\$140,000); DAILIES MUST HAVE A MINIMUM CAPITAL OF 500,000 DINARS WITHIN A THREE-MONTH PERIOD IN ORDER TO PUBLISH, A SEVENFOLD INCREASE FROM THE PREVIOUS LAW (ARTICLE 13);
- PUBLICATIONS "REFRAIN FROM PUBLISHING ANYTHING THAT CONFLICTS WITH THE PRINCIPLES OF FREEDOM, NATIONAL RESPONSIBILITY, HUMAN RIGHTS AND VALUES OF THE ARAB AND ISLAMIC NATION" (ARTICLE 5); AND
- PERIODICALS [WHICH ARE ALSO DEFINED IN A WAY THAT COULD INCLUDE ONLINE PUBLICATIONS] REFRAIN FROM PUBLISHING ANY MATERIALS CONTAINING CONTENT DEEMED OBJECTIONABLE, INCLUDING ANYTHING THAT "DISPARAGES THE KING AND THE ROYAL FAMILY...INFRINGES ON THE JUDICIARY OR UNDERMINES ITS INDEPENDENCE...[AND THAT] ENCOURAGES PERVERSION OR LEADS TO MORAL CORRUPTION" (ARTICLE 37).

VIOLATIONS OF ARTICLE 37 MAKE A PERIODICAL SUBJECT TO FINES OF NOT LESS THAN 5,000 DINARS (ARTICLE 47) AND POSSIBLE COURT-ORDERED CLOSURE (ARTICLE 50). AS OF MAY 1999, THE PRESS AND PUBLICATIONS LAW HAD BEEN INVOKED ONLY ONCE TO SUSPEND A PRINT PUBLICATION;³¹ ITS EFFECT ON ONLINE MEDIA REMAINED UNCLEAR.

Morocco

THE GOVERNMENT OF MOROCCO DOES NOT RESTRICT ACCESS TO THE INTERNET OR CENSOR CONTENT, ACCORDING TO SEVERAL INTERNET USERS INTERVIEWED IN MOROCCO. ACCOUNTS ARE EASILY OBTAINED FROM DOZENS OF PRIVATE SERVICE PROVIDERS, AND USERS CAN ACCESS THE UNFILTERED WORLD WIDE WEB FROM HOME, THE OFFICE, OR ONE OF MANY CYBERCAFÉS OPERATING IN THE BIG CITIES.

³¹ A COURT OF FIRST INSTANCE SUSPENDED AL-MAJID WEEKLY ON FEBRUARY 14, 1999. PUBLICATION RESUMED AFTER AN APPEALS COURT OVERTURNED THE SUSPENSION, BUT THE CHARGES AGAINST THE WEEKLY WERE NOT DROPPED.

Yet Internet use has grown slowly since it was introduced in late 1995. Contrary to official claims of more than 40,000 regular Internet users in a country of 29 million,⁹² the private Internet Association estimated the number of subscribers at 8,000 and the number of regular users at 12,000.⁹³ According to the association's president, Chakib Lahrichi, the slow growth is due not to government restrictions but rather to high costs for users, the absence of a national policy to promote Internet development, and unfair advantages enjoyed by the state-controlled telecommunications company Hissalat al-Maghrib (IAM) in its competition with private ISPs.⁹⁴

In early 1999, Internet access in Morocco cost about U.S. \$40-50 per month for a subscription that included fifteen hours online plus the cost of the telephone connection (approximately \$2 per hour). This cost was quite high for a country with one of the region's lowest per capita gross national products.⁹⁵ By 1999 the average subscriptions had dropped to about \$20 per month for unlimited access, with telephone charges remaining at about \$2 per hour.

⁹² The web site of the state-controlled Hissalat al-Maghrib telecommunications utility, <<http://onf.net.ma/>>, accessed May 12, 1999, claimed "more than 40,000 regular users in Morocco."

⁹³ E-mail communication from association president Chakib Lahrichi to Human Rights Watch, May 12, 1999.

⁹⁴ Interview with Human Rights Watch, Casablanca, April 30, 1999 and e-mail to Human Rights Watch, May 12, 1999. See also Ghassan Khaber, "Internet au Maroc: Deux ans et toujours à tâtonner," *L'Économiste* (Morocco), January 15, 1999.

⁹⁵ Morocco's GNP per capita was U.S.\$1,250 in 1997, according to The World Bank, *World Development Report, 1999/99*, p.191.

Lahrichi, who heads a major Casablanca-based private ISP called L&L Technologies, pointed out that Internet growth was impeded by the structure of telecommunications in the country. Private ISPs, he said, must use the lines and international gateway maintained by IAM. For the services it provides them, IAM "imposed whatever prices it wants" while competing with them as an ISP itself.

Lahrichi said, however, that he was aware of no government-imposed blocking or filtering of web pages, newsgroups, or e-mail. ISPs provided Internet access for anyone who could pay for it and were not required by the government to furnish any information about their customers. With respect to Morocco's cybercafés, Lahrichi said anyone could open one and he had not heard of any being the object of government pressure or surveillance.

Karl Stanzick, who manages an ISP called MIDS (Morocco Trade and Development Services) in Rabat, said "there is no 'usage contract' which needs to be signed or agreed to by the Internet subscriber whether purchasing an hour in the cybercafé, a dial-up account, or a leased line." Stanzick added that no government approval is required to obtain an Internet account or post a web site, and "all Internet subscribers in Morocco can be completely anonymous if they wish." He said the authorities have not imposed on ISPs any form of legal liability for materials they carry, and he was unaware of any ISP that had been punished for "objectionable" content. Stanzick remarked, however, that the "red lines" that inhibit political commentary in traditional media—the taboos on questioning the institution of the monarchy and Morocco's claim to the Western Sahara, and on "insulting" the King or Islam—also limit what Moroccans are willing to post in public chat-rooms and electronic bulletin boards.⁹⁶

The owner of an Internet café in a major Moroccan city, who requested anonymity, said that there had been no interference by authorities concerning what Internet users could do while at the establishment. He said clients could access anything they wished. A sample web search at the café for pro-Polissario⁹⁷ perspectives on the Western Sahara conflict turned up many sites, such as <www.arsd.org>, containing material that would never appear in the Moroccan print or broadcast media.

The only instance of censorship that the café had experienced occurred in February 1997, when the owner said he received a written order from the regional police headquarters warning him that a particular compact disc software program entitled "3D Atlas" was banned in Morocco. Although the order did not explain the reason for the prohibition, the owner said he had been given to understand that it was due to the way that this software presented the issue of sovereignty over the Western Sahara.

⁹⁶ E-mail communications to Human Rights Watch, May 21, 1998 and January 12, 1999.

⁹⁷ The Popular Front for the Liberation of Saquia el-Hamra and Rio de Oro, known as the Polisario Front, is the Western Saharan liberation movement. Morocco has asserted sovereignty over the territory and has been fighting a war against the Polisario since the mid-1970s.

ALTHOUGH THE GOVERNMENT OF MOROCCO DID NOT REPLY TO HUMAN RIGHTS WATCH'S WRITTEN QUESTIONS ABOUT INTERNET POLICIES, IT FORWARDED IN JUNE 1999 A FACT-SHEET ABOUT INTERNET USE IN THE KINGDOM. IT STATED THAT SIXTEEN GOVERNMENT MINISTRIES AND AGENCIES MAINTAIN WEB SITES AND SEVEN MOROCCAN NEWSPAPERS ARE ONLINE.⁹⁹

Saudi Arabia

IN JANUARY 1999, SAUDI ARABIA BEGAN ALLOWING ITS PUBLIC TO ACCESS THE INTERNET THROUGH LOCAL SERVICE PROVIDERS. IT DID SO WHILE PROMISING TO IMPLEMENT WHAT WOULD BE THE REGION'S MOST AMBITIOUS PLAN TO BLOCK THE FLOW OF "UNDESIRABLE" DATA ONLINE.

⁹⁹ THE FRENCH EMBASSY IN RABAT MAINTAINS A HANDY DIRECTORY OF ONLINE ADDRESSES IN MOROCCO, AT <www.ambafrance-ma.org/public/webmaroc.htm>.

Saudi Arabia has had an Internet connection since 1994, but restricted its use to state academic, medical, and research institutions. Saudi citizens and residents were free, however, to purchase computers and modems, could connect to the Internet through dial-up service to foreign ISPs, and launch web sites on foreign servers. But international calls to ISPs were expensive: to Bahrain the charge was U.S. \$0.60-0.80 per minute, and to the U.S. and Europe \$1.70-\$2.10 per minute. Still, according to one estimate, some 30,000 Saudis were accessing the Internet in this fashion.⁹⁹ The Saudi public could also subscribe to local networks such as al-Naseej (<www.naseej.com.sa>), which provided domestic and international e-mail, links to domestic databases and "chat rooms" for its own subscribers—but no access to the World Wide Web.

Although state institutions were first connected to the Internet in 1994 and King Fahd had approved public Internet access in 1997, it was not until January 1999 that local ISPs began connecting ordinary citizens. This delay was due in large part to the self-proclaimed determination of authorities to establish a system for controlling the flow of information online.

Officials of the Saudi government and the King Abdul-Aziz City for Science and Technology (KACST)—the Riyadh-based state institution charged with coordinating Internet policy—declined to respond to repeated written, phone, and e-mail invitations from Human Rights Watch to provide information. However, they made their intention to exercise control over Internet content clear in numerous press interviews. Saleh Abdulrahman Al-'Adhel, president of the KACST, said in February 1998:

⁹⁹ "Saudi Arabia ready to cruise the information superhighway," Agence France-Presse, July 15, 1998.

A STANDING COMMITTEE HAS BEEN FORMED AND APPROVED BY THE GOVERNMENT TO PROTECT SOCIETY FROM MATERIAL ON THE INTERNET THAT VIOLATES ISLAM OR ENCRUCHESES ON OUR TRADITIONS AND CULTURE. THIS COMMITTEE WILL DETERMINE WHICH SITES ARE IMMORAL, SUCH AS PORNOGRAPHIC SITES AND OTHERS, AND WILL BAR SUBSCRIBERS FROM ENTERING SUCH SITES. THERE ARE MANY BAD THINGS ON INTERNET. THAT IS WHY WE HAVE CREATED A MECHANISM TO PREVENT SUCH THINGS FROM REACHING OUR SOCIETY SO THAT A HOME SUBSCRIBER TO THIS SERVICE CAN BE REASSURED. WE HAVE PROGRAMS, SOFTWARE, AND HARDWARE THAT PREVENT THE ENTRY OF MATERIAL THAT CORRUPTS OR THAT HARMS OUR MUSLIM VALUES, TRADITION, AND CULTURE. WE ALSO CREATED A "FIRE WALL" OR BARRIER TO PREVENT OTHER QUARTERS FROM BREACHING OUR SITES. THAT IS WHY WE HAVE NOT RUSHED INTO PROVIDING THIS SERVICE. WE FIRST WANT TO MAKE SURE WE ELIMINATE ALL NEGATIVE ASPECTS OF THE INTERNET.¹⁰⁰

THAT OBJECTIVE WAS ENDORSED EARLY ON BY SAUDI ARABIA'S COUNCIL OF MINISTERS WHEN IT CALLED FOR A FIRE WALL, MAINTAINED BY THE KACST, TO KEEP THE PUBLIC FROM ACCESSING "INAPPROPRIATE" INFORMATION.¹⁰¹ THE COUNCIL ALSO PREPARED A SET OF BROAD AND VAGUELY DEFINED RESTRICTIONS ON INTERNET CONTENT AND USAGE. ITS DECISION NUMBER 163, MADE PUBLIC IN MAY 1999, REQUIRES ISPs AND USERS TO REFRAIN FROM "USING THE NETWORK FOR ILLEGITIMATE PURPOSES SUCH AS, FOR EXAMPLE, PORNOGRAPHY AND GAMBLING;...CARRYING OUT ANY ACTIVITIES VIOLATING THE SOCIAL, CULTURAL, POLITICAL,

¹⁰⁰ QUOTED IN *UKAZ* NEWSPAPER, FEBRUARY 24, 1999, AS REPORTED IN FBIS, FEBRUARY 27, 1999.

¹⁰¹ THE MOSAIC GROUP, *THE GLOBAL DIFFUSION OF THE INTERNET PROJECT: AN INITIAL INDUCTIVE STUDY*, MARCH 1999, P. 216, OR <www.igsd.com/gdi97/gdi97.html>. AN UPDATED VERSION, DATED FEBRUARY 1999, OF THE *INDUCTIVE STUDY'S* CHAPTER ON SAUDI ARABIA CAN BE FOUND AT <www.igsd.com/gdiff/gdiff4>. THE TERM "FIRE WALL" CONNOTES VARIOUS TOOLS THAT RESTRICT USERS' ACCESS TO ONLINE DATA, EITHER IN PROPRIETARY SITES OR ON THE INTERNET. IT CAN BE SET UP AS A SECURITY DEVICE TO PREVENT UNAUTHORIZED ACCESS TO COMPUTER SYSTEMS OR AS A CENSORSHIP DEVICE TO BLOCK USER ACCESS TO ONLINE MATERIALS THAT A GOVERNMENT OR FIRE-WALL OPERATOR SEEKS TO PLACE OFF-LIMITS.

MEDIA, ECONOMIC, AND RELIGIOUS VALUES OF THE KINGDOM OF SAUDI ARABIA; SENDING OR RECEIVING CODED INFORMATION UNLESS AFTER OBTAINING THE NECESSARY LICENSES FROM THE ADMINISTRATION OF THE NETWORK IN QUESTION; [AND] INTRODUCING OTHERS INTO THE USAGE ACCOUNTS OR BRIEFING THEM ON THE SECRET NUMBER OF THE USER."¹⁰²

¹⁰² QUOTED IN *AL-JAZIRA* NEWSPAPER, MAY 6, 1998, AS REPORTED IN FBI'S, MAY 12, 1998.

Authorities have divulged few details of the technical means and criteria used to block content. According to one press report, "Industry insiders claim King Abdul-Aziz City for Science and Technology will simply provide a list of desirable sites, officially sanctioned by an internal committee. All other sites will be banned by default. In other words, the user will not be able to type in the URL of any site that he/she wants to visit, but rather only be able to pick from an officially sanctioned list."¹⁰³ If accurate, this would be the world's most restrictive regime of web-site filtering. The London-based daily *AL-SHARQ AL-AWSAF* reported that the Saudis planned to contract with U.S. firms to bolster their censorship efforts by furnishing on a continuous basis the addresses of web sites deemed offensive.¹⁰⁴

Saudi Arabia allows private ISPs. In November 1999 the government approved applications from some forty companies seeking to provide Internet services. However, all ISPs operating in the Kingdom are to be linked to a main server at the KACST, which has the country's sole gateway to the World Wide Web.¹⁰⁵ This structure would certainly facilitate any possible efforts by the government to monitor and limit Internet use and content.

Two months after local ISPs began offering access, Al-'Adhel affirmed that the KACST was "blocking undesirable web sites" by using what he called "very fast computer programs." He denied that the KACST had prohibited any applications, such as chat services—"unless [they were] linked to pornographic sites."¹⁰⁶

¹⁰³ IT NEWS, NOVEMBER 4, 1999, <www.difnet.co.ae/html/newsnov/newsnov0199.html>.

¹⁰⁴ "Internet Service in the Arab World," *AL-SHARQ AL-AWSAF*, OCTOBER 4, 1999, AS REPORTED IN FBIS, OCTOBER 29, 1999.

¹⁰⁵ THE REGULATIONS ON ISPs FORBID THEM FROM ESTABLISHING ANY LINKAGE TO THE INTERNET EXCEPT VIA THE KACST. THE RULES WERE PUBLISHED IN THE MAY 6, 1999 *AL-JAZIRA* DAILY, AS REPORTED IN FBIS, MAY 12, 1999.

¹⁰⁶ NASSER SALIH AL-SARAMI, "PROBLEMS AND POSSIBILITIES: INTERNET IN THE KINGDOM," *SAUDI GAZETTE*, MARCH 13, 1999.

ALTHOUGH OFFICIAL EXPLANATIONS OF CONTENT FILTERING HAVE FOCUSED ON MATERIALS DEEMED OFFENSIVE TO CONSERVATIVE MUSLIM SENSIBILITIES, SAUDI BLOCKING APPARENTLY EXTENDS TO POLITICAL SITES. IN EARLY 1999, THE SITE OF AT LEAST ONE EXILED DISSIDENT GROUP, THE COMMITTEE AGAINST CORRUPTION IN SAUDI ARABIA (<www.saudhouse.com>), WAS REPORTEDLY BLOCKED.

USERS WHO ATTEMPT TO ACCESS BANNED SITES REPORTEDLY RECEIVE WARNINGS ON THEIR COMPUTER SCREENS THAT THEIR ACCESS ATTEMPTS ARE BEING LOGGED.¹⁰⁷ SAUDI AUTHORITIES HAVE ALSO TRIED TO THWART USER EFFORTS TO CIRCUMVENT CENSORSHIP. THE URL OF A POPULAR WEB-BASED ANTI-CENSORSHIP PROXY SERVER, OSIRIS, IS BLOCKED IN THE KINGDOM, ALONG WITH AT LEAST THREE "MIRROR" SITES, ACCORDING TO BRIAN RISTUCCIA, WHO MANAGES THE SITE.¹⁰⁸ AND A WEB SITE OFFERING ANONYMIZING SERVICES, <www.anonymizer.com>, IS ALSO BLOCKED, ACCORDING TO THE COMPANY'S PRESIDENT, LANCE COTTRELL.¹⁰⁹

THE PRICING STRUCTURE FOR INTERNET ACCOUNTS THAT WAS ANNOUNCED BY THE KACST FOR ISP CHARGES APPEARS MODERATE TO HIGH, DEPENDING ON WHETHER THE ISPS CHOOSE TO OFFER RATES CLOSER TO THE LOW OR HIGH END OF THE PERMISSIBLE RANGE SET BY THE KACST. SAUDI NEWSPAPERS ON NOVEMBER 10, 1999 QUOTED KACST OFFICIALS SAYING THEY HAD AGREED TO A MINIMUM ISP CHARGE OF 1.5 RIYALS AN HOUR (1 RIYAL EQUALS U.S.\$0.27) AND A MAXIMUM OF 4.5 RIYALS, ALONG WITH A FIXED MONTHLY CHARGE OF BETWEEN 100 AND 150 RIYALS. AN ADDITIONAL DIAL-UP CHARGE OF 4.5 RIYALS PER HOUR WOULD BE PAID TO SAUDI TELECOM.¹¹⁰ (SAUDI TELECOM IS A STATE MONOPOLY, ALTHOUGH THE FIRST STEPS TOWARD

¹⁰⁷ JEHL, "THE INTERNET'S 'OPEN SESAME,'" *NEW YORK TIMES*.

¹⁰⁸ E-MAIL COMMUNICATION FROM BRIAN RISTUCCIA TO HUMAN RIGHTS WATCH, JANUARY 7, 1999 AND MARCH 11, 1999.

¹⁰⁹ COTTRELL, "COMMERCIAL ANONYMITY."

¹¹⁰ "SAUDI SETS LIMITS TO INTERNET PROVIDER CHARGES," *Reuters*, November 10, 1998.

privatizing it were taken in 1999.) Thus, a light user, one who spends five hours online per month, would pay a monthly rate of between U.S. \$36-\$44.

Syria

Despite an online connection established in 1997 and frequent pro-Internet statements, Syria remains the only connected country in the region that has yet to allow its public local access to the Internet. But a few thousand modems are said to be in Syrian hands, allowing those who have access to them to maintain Internet accounts with ISPs in Lebanon and elsewhere.¹¹¹ Syrians who are able to travel to neighboring Jordan or Lebanon can patronize cybercafés; none exist in Syria.

¹¹¹ JOSEPH CONTRERAS, "THE INFORMATION AGE DAWNS, CHAMPIONED BY ASSAD'S SON," *NEWSWEEK*, APRIL 26, 1999.

THE GOVERNMENT OF PRESIDENT HAFEZ AL-ASAD DID NOT RESPOND TO HUMAN RIGHTS WATCH'S LETTER REQUESTING INFORMATION ON INTERNET POLICIES. ITS GO-SLOW APPROACH IS CONSISTENT HOWEVER WITH ITS EFFORTS TO SUPPRESS ALL FORMS OF EXPRESSION DEEMED CRITICAL OF HOW THE COUNTRY IS GOVERNED. ALL NEWSPAPERS AND BROADCAST MEDIA ARE TIGHTLY CONTROLLED, AND HUNDREDS OF POLITICAL PRISONERS REMAIN BEHIND BARS, MANY OF THEM SERVING LONG TERMS FOR PEACEFUL DISSENT.¹¹²

OFFICIAL DISCOURSE ABOUT THE INTERNET HAS BEEN AMBIVALENT, FAVORABLE TO ITS POTENTIAL AS A TOOL OF COMMUNICATION WHILE MINDFUL OF ITS PURPORTED SOCIAL DANGERS. A FEBRUARY 1999 ARTICLE IN THE OFFICIAL *TISHRIN* DAILY ADVOCATED AN ARAB STRATEGY TO DEVELOP INTERNET USE IN ORDER TO COUNTERACT THE HEAVY INTERNET PRESENCE OF ISRAELI SOURCES AND VIEWPOINTS. THE AUTHOR CALLED FOR "PREPAR[ING] NATIONAL AND ARAB PLANS TO INTRODUCE THE INTERNET CULTURE TO ALL PEOPLE" AND PROVID[ING] INTERNET CONNECTIONS AT SYMBOLIC RATES."¹¹³ SINCE 1997, SOME OFFICIAL AND SEMI-OFFICIAL SYRIAN INSTITUTIONS HAVE BEEN LINKED TO THE INTERNET. SOME HAVE ESTABLISHED A PRESENCE ON THE WEB, INCLUDING THE SYRIAN ARAB NEWS AGENCY (<www.sana.org>), *TISHRIN* DAILY (<www.tishreen.com>), AND THE SYRIAN COMPUTER SOCIETY (<www.scs-syria.org>).

SYRIA'S MOST PROMINENT ADVOCATE OF THE INTERNET IS BASHAR AL-ASAD, THE PRESIDENT'S SON. HE CHAIRS THE SYRIAN COMPUTER SOCIETY. ACCORDING TO ONE NEWS REPORT, BASHAR'S POSITION IN FAVOR OF PUBLIC ACCESS TO THE INTERNET HAS BEEN OPPOSED BY SECURITY AND INTELLIGENCE OFFICIALS.¹¹⁴

¹¹² SEE THE SYRIA CHAPTER IN HUMAN RIGHTS WATCH, *HUMAN RIGHTS WATCH WORLD REPORT 1999* (NEW YORK: HUMAN RIGHTS WATCH, 1999), PP. 372-376, AND REPORTERS SANS FRONTIÈRES, "JOURNALISTS TORTURED IN SYRIA," MARCH 1999.

¹¹³ HUSAYN AL-IBRAHIM, "THE INTERNET AND INFORMATICS IN THE ARAB-ISRAELI CONFLICT," *TISHRIN*, FEBRUARY 23, 1999, AS REPORTED IN FBIS, MARCH 1, 1999.

¹¹⁴ DOUGLAS JELL, "IN SYRIA, ONLY THE POPULATION IS GROWING," *NEW YORK TIMES*, JANUARY 25, 1999.

A spokesman for the Syrian Computer Society, Saadallah Agha al-Kalaa, justified the slow approach to extending access beyond state institutions. "Our problem is...we are a traditional society, and we have to know if there is something that cannot fit with our society. We have to make it safe." He added, "We want to have Internet with a minimum of problems, so the solution was to go by stages. Where the need is most important, in universities, centers of research, ministries of economy...all these sites are connected now." Kalaa insisted that the government's reluctance to open up Syria to the Internet reflected social concern about Internet content rather than political fears about the free exchange of information.¹⁵

In an article sympathetically explaining Syria's "cautious" approach to the Internet, Amr Salem, a co-founder of the SCS, wrote:

IN ORDER FOR PRESIDENT ASSAD TO FEEL COMFORTABLE PROMOTING A PARTICULAR TECHNOLOGY, IT MUST MEET THE FOLLOWING CRITERIA:

1. IT SHOULD BENEFIT THE MAJORITY OF THE SYRIAN PEOPLE. TECHNOLOGY GEARED TOWARD THE ELITE IS NOT FAVORED BECAUSE SUCH PEOPLE HAVE THE RESOURCES AND MEANS TO GET WHAT THEY WANT WITHOUT GOVERNMENT ASSISTANCE.
2. IT SHOULD NOT DISRUPT THE SOCIAL STRUCTURE OR ADVERSELY AFFECT THE MIDDLE CLASS, AND MUST BE WITHIN THE MEANS OF THE MASSES.
3. IT SHOULD HAVE A DIRECT IMPACT ON SYRIA'S OVERALL SOCIAL AND ECONOMIC DEVELOPMENT.
4. IT SHOULD NOT JEOPARDIZE SYRIAN INDEPENDENCE OR SECURITY CONCERNS.¹⁶

ACCORDING TO ONE NEWS REPORT, THE FEW SYRIANS WHO HAVE ACCESS TO THE INTERNET BECAUSE THEY WORK AT CONNECTED STATE INSTITUTIONS DO NOT HAVE UNFETTERED ACCESS: SYRIA'S SOLE SERVICE PROVIDER, THE MONOPOLY SYRIAN TELECOMMUNICATIONS ESTABLISHMENT (STE), BLOCKS ACCESS TO WEB

¹⁵ JACK REDDEN, "INTERNET ARRIVES IN SYRIA, BUT NOT WITHOUT LIMITS," REUTERS, JULY 10, 1998. AN E-MAIL SENT BY HUMAN RIGHTS WATCH TO THE SCS SEEKING COMMENT ON THE REUTERS STORY WENT UNANSWERED.

¹⁶ AMR SALEM, "SYRIA'S CAUTIOUS EMBRACE," *MIDDLE EAST INSIGHT*, MARCH-APRIL 1999, PP. 49-50.

SITES CONTAINING INFORMATION OR PICTURES DEEMED OFFENSIVE.¹⁷⁷ HUMAN RIGHTS WATCH HAS NO INFORMATION CONCERNING THE TYPE OF CONTENT THAT IS BLOCKED. AS NOTED ABOVE, THE SYRIAN GOVERNMENT AND THE SYRIAN COMPUTER SOCIETY DID NOT RESPOND TO WRITTEN QUERIES FROM HUMAN RIGHTS WATCH CONCERNING RESTRICTIONS ON WEB ACCESS AND CONTENT.

¹⁷⁷ "INTERNET SERVICE IN THE ARAB WORLD," *AL-SHARQ AL-AWSAH*, OCTOBER 6, 1999, AS REPORTED IN FBIS, OCTOBER 29, 1999.

IN EARLY 1999 THERE WERE ONCE AGAIN PRESS REPORTS THAT PUBLIC ACCESS WAS IMMINENT. Reuters reported that a public domestic e-mail service would be made available on a limited basis in February, but would be via a special server at the state telecommunications center that "would allow control of incoming and outgoing services, including the ability to block contact with destinations regarded as undesirable."¹¹⁸ As of May 1999, public access was still unavailable.

Tunisia

THE RELATIVE LENGTH OF THIS SECTION SHOULD NOT BE TAKEN TO MEAN THAT TUNISIA'S RESTRICTIONS ON THE INTERNET ARE MORE ONEROUS THAN ELSEWHERE. IT IS A REFLECTION, RATHER, OF THE FACT THAT TUNISIA HAS THE REGION'S MOST DETAILED INTERNET LEGISLATION, IT HAS EXPLICITLY EXTENDED ITS PRESS LAW TO COVER THE INTERNET, AND THE GOVERNMENT HAS PROVIDED HUMAN RIGHTS WATCH WITH MUCH INFORMATION ON WHICH TO COMMENT.

TUNISIAN POLICY REFLECTS DEEP AMBIVALENCE TOWARD THE INTERNET. PRESIDENT ZINE AL-ABIDINE BEN ALI HAS EXTOLLED THE IMPORTANCE OF DEVELOPING INFORMATION TECHNOLOGIES, INCLUDING THE INTERNET, AND OF MAKING IT WIDELY ACCESSIBLE.¹¹⁹ OFFICIAL AGENCIES HAVE AN ACTIVE PRESENCE ON THE WORLD WIDE WEB (SEE <WWW.MINISTERES.TN>), AND TUNISIAN TELEVISION AND RADIO ARE BROADCAST LIVE ONLINE (<WWW.TUNISIA.TV.COM> AND <WWW.RADIOTUNIS.COM>). THE GOVERNMENT HAS BEEN IMPROVING THE INTERNET INFRASTRUCTURE BY WIDENING THE BANDWIDTH, AMONG OTHER MEASURES. THE RATES CHARGED FOR INTERNET ACCESS AND PHONE USE HAVE BEEN DROPPING, ALONG WITH CUSTOMS DUTIES ON IMPORTED COMPUTER EQUIPMENT, MAKING INTERNET ACCESS MORE AFFORDABLE.

TUNISIAN AUTHORITIES SAY THE COUNTRY'S INTERNET-SPECIFIC LEGISLATION IS DESIGNED TO "PROMOTE" THE DELIVERY OF INTERNET SERVICES AND "PREPARE TUNISIA FOR THE AGE OF THE INFORMATION SOCIETY." THE LEGISLATION AIMS TO "FURNISH ACCESS TO INTERNET SERVICES TO ALL WHO WANT IT, AT THE SAME QUALITY AND THE SAME PRICE" AND TO "STIMULATE THE PRIVATE SECTOR, WITHIN A FRAMEWORK OF LOYAL COMPETITION, TO COMMERCIALIZE INTERNET ACCESS SERVICES AND DEVELOP WEB-SITE HOSTING CAPACITY." THE GOVERNMENT ALSO "AIMS TO CONNECT ALL UNIVERSITY AND SCIENTIFIC RESEARCH INSTITUTIONS TO THE INTERNET, TO BE FOLLOWED IN STAGES BY THE CONNECTION OF HIGH SCHOOLS

¹¹⁸ "SYRIA PLANS CONTROLLED E-MAIL SERVICE," REUTERS, JANUARY 6, 1999.

¹¹⁹ UNLESS OTHERWISE NOTED, ALL CITATIONS ARE FROM THE REPLY BY THE TUNISIAN GOVERNMENT TO HUMAN RIGHTS WATCH'S QUESTIONS, REPRINTED IN APPENDIX C. IT WAS TRANSLATED FROM FRENCH BY HUMAN RIGHTS WATCH.

("LYCÉES ET COLLÈGES") BETWEEN NOW AND THE END OF THE CURRENT [FIVE-YEAR] PLAN [2001], WITH THE INTENTION OF CONNECTING PRIMARY SCHOOLS TO THIS NETWORK IN THE SUBSEQUENT STAGE."

WHILE TUNISIA'S INTERNET REGULATIONS ESTABLISH STANDARDS AND RULES FOR AN EMERGING COMMERCIAL SECTOR, THEY ALSO REFLECT THE GOVERNMENT'S RESTRICTIVE APPROACH TO FREEDOM OF EXPRESSION AND INTOLERANCE OF DISSENT. IN TUNISIA, ALL NEWS MEDIA PROMOTE THE OFFICIAL LINE AND AVOID NEWS AND COMMENTARY THAT IMPLY CRITICISM OF GOVERNMENT POLICIES. SMALLER PUBLICATIONS HAVE ONLY SLIGHTLY MORE LEeway. POLITICAL AND HUMAN RIGHTS ACTIVISTS WHO HAVE CRITICIZED REPRESSIVE MEASURES HAVE BEEN JAILED, PENALIZED AT THEIR WORKPLACES, PREVENTED FROM TRAVELING ABROAD, OR OTHERWISE HARASSED. PERVERSIVE POLICE SURVEILLANCE OF ACTIVISTS, EX-PRISONERS, AND THEIR FAMILIES REINFORCES A CLIMATE OF FEAR AND SELF-CENSORSHIP.¹⁰⁰

TUNISIA'S PRESS CODE CONTAINS MANY ARTICLES THAT RESTRICT THE CONTENT OF WHAT MAY BE SAID OR PUBLISHED. ARTICLE 62 FORBIDS THE DISTRIBUTION, SALE, DISPLAY, OR POSSESSION OF "LEAFLETS, PUBLICATIONS, OR BOOKS, OF DOMESTIC OR OF FOREIGN ORIGIN, THAT ARE OF A NATURE THAT COULD DISTURB PUBLIC ORDER AND GOOD MORALS." THE PROVISIONS MOST FREQUENTLY USED TO PUNISH CRITICAL SPEECH ARE ARTICLE 49, WHICH CRIMINALIZES THE DISSEMINATION OF "FALSE" INFORMATION, AND ARTICLES 50-53, WHICH DEAL WITH DEFAMATION. ARTICLE 49 STATES:

THE PUBLICATION, DISSEMINATION OR REPRODUCTION BY ANY MEANS OF FALSE NEWS, INFORMATION WHICH HAS BEEN FABRICATED, FALSIFIED OR WRONGLY ATTRIBUTED TO OTHERS, IF MADE IN BAD FAITH AND IF IT HAS EITHER DISTURBED OR IS LIKELY TO DISTURB PUBLIC ORDER, MAY BE PUNISHED BY IMPRISONMENT OF TWO MONTHS TO THREE YEARS AND/OR A FINE OF 100-2,000 DINARS [EQUIVALENT TO U.S. \$93-1,960].

ARTICLE 50 STATES THAT DEFAMATION HAS OCCURRED IF THERE IS "A PUBLIC ALLEGATION OR ATTRIBUTION OF A FACT THAT HARMS THE HONOR OR ESTEEM (*CONSIDÉRATION*) OF A PERSON OR STATE AGENCY TO WHOM THE FACT WAS ATTRIBUTED." DEFAMATION IS PUNISHABLE BY UP TO THREE YEARS IN PRISON AND A FINE OF UP TO 1,200 DINARS IF THE OFFENDING MATERIAL IS PUBLISHED "DIRECTLY OR BY MEANS OF REPRODUCTION" (ARTICLE 50). THE CODE SPECIFIES VARIOUS PUBLIC ENTITIES THAT CAN BE THUS DEFAMED, INCLUDING "THE PUBLIC ORDER, THE COURTS, THE GROUND, SEA AND AIR FORCES, PUBLIC

¹⁰⁰ FOR GENERAL INFORMATION ABOUT THE STATE OF FREE EXPRESSION, SEE ARTICLE 19, *SURVEILLANCE AND REPRESSION: FREEDOM OF EXPRESSION IN TUNISIA* (LONDON: ARTICLE 19, MAY 1999); HUMAN RIGHTS WATCH, *HUMAN RIGHTS WATCH WORLD REPORT 1999* (NEW YORK: HUMAN RIGHTS WATCH, DECEMBER 1999); AND THE U.S. DEPARTMENT OF STATE'S *COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES FOR 1999*.

AGENCIES AND PUBLIC ADMINISTRATIONS." DEFAMATION IS PUNISHABLE BY THE SAME PENALTIES IF IT IS COMMITTED AGAINST ONE OR MORE "MEMBERS OF THE GOVERNMENT, ONE OR MORE DEPUTIES, CIVIL SERVANTS," AND OTHER PUBLIC SERVANTS "BY VIRTUE OF THEIR FUNCTIONS OR THEIR STATUS." THE TRUTH OF THE ALLEGATION CAN BE USED AS A DEFENSE, BUT NOT IN ALL SITUATIONS.

THE USE OF THESE ARTICLES TO PROSECUTE JOURNALISTS AND OTHERS ILLUSTRATES WHAT THE ORGANIZATION ARTICLE 19 CHARACTERIZED AS "THE STATE USING THE LAW TO PREVENT PUBLIC DISCUSSION OF MATTERS OF GREAT PUBLIC IMPORT BUT WHICH ARE IN SOME WAY CRITICAL OF THE GOVERNMENT'S PERFORMANCE."¹²¹ ONE EXAMPLE IS THE THREE-YEAR PRISON SENTENCE IMPOSED ON HUMAN RIGHTS ACTIVIST KHEMAIS KSTLA FOR A COMMUNIQUÉ HE DISTRIBUTED IN SEPTEMBER 1997 DENOUNCING GOVERNMENT REPRESSION.

A STATE AGENCY, THE AGENCE TUNISIENNE D'INTERNET (ATI), COORDINATES INTERNET POLICIES AND SERVICES AND ACTS AS A KIND OF SUPER-ISP. IT LEASES INTERNET ACCESS TO SEVERAL PRIVATE ISPs, INCLUDING TWO THAT ARE LICENSED TO OFFER INTERNET SERVICES TO THE PRIVATE SECTOR AND INDIVIDUALS, GLOBAL NET (<WWW.GNET.TN>) AND PLANET. THESE TWO COMPANIES ARE REPORTEDLY CONTROLLED BY PERSONS CLOSE TO THE PRESIDENT. ALL PRIVATE ISPs MERELY RETAIL INTERNET ACCESS TO CUSTOMERS; ALL COMMUNICATIONS, DOMESTIC AND INTERNATIONAL, REPORTEDLY GO THROUGH THE ATI AND THE STATE TELECOMMUNICATIONS NETWORK. THE ATI MAINTAINS CONTROL OVER ALL OF THE PROTOCOLS AND THE COUNTRY'S ONLY INTERNATIONAL GATEWAY.

THE MAIN PIECE OF LEGISLATION GOVERNING THE INTERNET IS A DECREE ISSUED ON MARCH 22, 1997, HEREINAFTER "THE INTERNET DECREE."¹²² IT FOLLOWED BY EIGHT DAYS A DECREE THAT COVERS TELECOMMUNICATIONS SERVICES MORE GENERALLY.¹²³

¹²¹ ARTICLE 19, *SURVEILLANCE AND REPRESSION: FREEDOM OF EXPRESSION IN TUNISIA* (LONDON: ARTICLE 19, MAY 1999), P. 71.

¹²² ARRÊTÉ DU MINISTRE DES COMMUNICATIONS DU 22 MARS 1997, PORTANT APPROBATION DU CAHIER DES CHARGES FIXANT LES CLAUSES PARTICULIÈRES À LA MISE EN ŒUVRE ET L'EXPLOITATION DES SERVICES À VALEUR AJOUTÉE DES TÉLÉCOMMUNICATIONS DE TYPE INTERNET.

¹²³ DÉCRET NO. 97-501 DU 14 MARS 1997 RELATIF AUX SERVICES À VALEUR AJOUTÉE DES TÉLÉCOMMUNICATIONS.

THE TELECOMMUNICATIONS DECREE PROVIDES THE FOLLOWING:

- THE PRESS CODE SHALL APPLY TO THE PRODUCTION, PROVISION, DISTRIBUTION AND STORING OF INFORMATION THROUGH TELECOMMUNICATION MEANS [INCLUDING THE INTERNET] (ARTICLE 1).
- ALL ISPs MUST OBTAIN A LICENSE FROM THE MINISTRY OF COMMUNICATIONS (ARTICLE 7).
- A "COMMISSION ON TELECOMMUNICATIONS SERVICES" SHALL REVIEW EACH APPLICATION TO OPERATE AN ISP COMPANY; THE COMMISSION INCLUDES REPRESENTATIVES FROM THE MINISTRIES OF DEFENSE AND INTERIOR, AS WELL AS OFFICIALS HOLDING POSTS RELATED TO COMMUNICATIONS, INFORMATION AND COMPUTER SCIENCES (ARTICLE 9).

THE INTERNET DECREE IMPOSES THE FOLLOWING RULES:

- EACH ISP MUST DESIGNATE A DIRECTOR WHO "ASSUMES RESPONSIBILITY...FOR THE CONTENT OF PAGES AND WEB PAGES AND SITES THAT THE ISP IS REQUESTED TO HOST ON ITS SERVERS (ARTICLE 9, PARAGRAPH 3). INTERNET USERS AND THOSE WHO MAINTAIN WEB SITES AND SERVERS ARE ALSO RESPONSIBLE FOR INFRINGEMENTS OF THE LAW (ARTICLE 9, PARAGRAPH 4);
- EACH ISP MUST SUBMIT, ON A MONTHLY BASIS, A LIST OF ITS INTERNET SUBSCRIBERS TO THE "PUBLIC OPERATOR" (THE STATE-RUN AIT) (ARTICLE 9, PARAGRAPH 5); IF THE ISP CLOSES DOWN OR STOPS PROVIDING SERVICES, IT MUST "WITHOUT DELAY" TURN OVER TO THE "PUBLIC OPERATOR" A COMPLETE SET OF ITS ARCHIVES ("L'ENSEMBLE DES SUPPORTS D'ARCHIVAGE") AS WELL AS THE MEANS TO READ IT (ARTICLE 9, PARAGRAPH 7).
- THE "DIRECTOR" IS TO MAINTAIN "CONSTANT OVERSIGHT" OF THE CONTENT ON THE ISP'S SERVERS, TO INSURE THAT NO INFORMATION REMAINS ON THE SYSTEM THAT IS CONTRARY TO "PUBLIC ORDER AND GOOD MORALS" ("L'ORDRE PUBLIC" AND "BONNES MŒURS," THE SAME PHRASES THAT ARE FOUND IN ARTICLE 62 OF THE PRESS CODE, WHICH PROVIDES FOR THE CONFISCATION OF PUBLICATIONS).

THE INTERNET DECREE ALSO BARS ENCRYPTION WITHOUT PRIOR APPROVAL FROM THE AUTHORITIES (ARTICLE 11). A SEPTEMBER 1997 DECREE ON ENCRYPTION REQUIRES THAT PERSONS OR SERVICE PROVIDERS WHO WISH TO ENCRYPT DATA MUST SUBMIT AN APPLICATION TO THE MINISTRY OF COMMUNICATIONS AND PROVIDE THE KEYS NEEDED TO DECRYPT THE DATA.¹²⁴ THE MINISTRY DECIDES ON THE APPLICATION AFTER CONSULTING THE COMMISSION ON TELECOMMUNICATIONS, CITED ABOVE.

THE CONTRACT THAT INSTITUTIONAL SUBSCRIBERS SIGN WHEN OBTAINING SERVICES FROM THE AIT IMPOSES FURTHER GOVERNMENT CONTROLS. MOST REMARKABLY, IT REQUIRES USERS TO SIGN THAT THEY WILL

¹²⁴ ARRÊTÉ DU MINISTRE DES COMMUNICATIONS DU 9 SEPTEMBRE 1997 FIXANT LES CONDITIONS D'UTILISATION DU CRYPTAGE DANS L'EXPLOITATION DES SERVICES À VALEUR AJOUTÉE DES TÉLÉCOMMUNICATIONS.

"USE THE INTERNET ONLY FOR SCIENTIFIC, TECHNOLOGICAL OR COMMERCIAL PURPOSES THAT ARE STRICTLY RELATED TO THE ACTIVITY OF THE CLIENT, IN STRICT CONFORMITY WITH THE RULES IN EFFECT." THE CONTRACT ALSO REQUIRES THAT CLIENTS:

- "DISCLOSE TO THE AIT ALL ACCOUNTS THAT HAVE BEEN OPENED FOR USERS AND THOSE HAVING ACCESS";
- "PREVENT REMOTE ACCESS TO ITS NETWORK BY EXTERNAL USERS WHO LACK PRIOR AUTHORIZATION FROM THE AIT"; AND
- "INFORM THE AIT OF ANY CHANGE IN ADDRESS, EQUIPMENT, AND USER."

THE AIT RESERVES THE RIGHT TO SUSPEND INTERNET SERVICE WITHOUT NOTICE IF THE SUBSCRIBER ENGAGES IN ANY USE THAT IS "IMPROPER OR CONTRARY TO THE CONDITIONS LAID OUT" IN THE CONTRACT. THE AGENCY ALSO HAS THE RIGHT UNDER THE CONTRACT TO CONDUCT SITE VISITS TO ENSURE THAT THE EQUIPMENT CONNECTED TO THE INTERNET IS BEING USED "IN CONFORMITY WITH THE RULES AND LAWS AS WELL AS TO ENSURE THEY ARE BEING USED PROPERLY." (EMBASSIES AND INTERNATIONAL INSTITUTIONS ARE EXEMPTED FROM THIS PROVISION.)

COMMENTARY ON TUNISIA'S LEGISLATION

Responsibility of ISP for content: THE IMPOSITION OF LEGAL RESPONSIBILITY ON THE ISP, AND SPECIFICALLY ON ITS DESIGNATED "RESPONSIBLE PERSON," FOR THE WEB SITES IT HOSTS, POSES A THREAT TO ONLINE FREEDOM OF EXPRESSION. IT DOES SO BY IMPOSING A REGULATORY BURDEN ON PROVIDERS EVEN THOUGH THEY CANNOT REALISTICALLY POLICE THE WEB SITES THEY HOST, MANY OF WHICH ARE REVISED DAILY BY THEIR AUTHORS. IF ENFORCED, THIS PROVISION IS LIKELY TO SLOW OR REDUCE THE FLOW OF DATA ONLINE.

THE GOVERNMENT, IN ITS LETTER TO HUMAN RIGHTS WATCH, STATES THAT ISPS ARE RESPONSIBLE ONLY FOR THE CONTENT OF WEB SITES BUT NOT FOR THE CONTENT OF E-MAIL MESSAGES OR NEWSGROUP POSTINGS. BUT RESPONSIBILITY FOR NEWSGROUP CONTENT SEEMS ENCOMPASSED BY THE SECTION OF THE INTERNET DECREE STIPULATING THAT THE ISP MUST ALLOW NOTHING TO "REMAIN" ON ITS SERVERS THAT HARMS "PUBLIC ORDER AND GOOD MORALS." THIS BROAD AND VAGUE WORDING SEEMS INTENDED TO COMPEL ISPS TO ERR ON THE SIDE OF CENSORING CONTENT SO AS NOT TO RUN AFOUL OF THE REGULATIONS.

FURNISHING LISTS OF SUBSCRIBERS TO THE GOVERNMENT. THE GOVERNMENT EXPLAINS THAT ISPS MUST SUBMIT MONTHLY THE NAMES OF ITS SUBSCRIBERS IN ORDER TO FACILITATE MAINTAINING A STATISTICAL BASE AND DIRECTORY OF INTERNET USERS. THE GOVERNMENT STATES THAT ISPS MUST OTHERWISE KEEP INFORMATION ABOUT USERS AND THEIR USAGE CONFIDENTIAL.

THE OBLIGATION TO FURNISH THE GOVERNMENT WITH SUBSCRIBER LISTS INFRINGES ON THE PRIVACY AND ANONYMITY RIGHTS OF INTERNET USERS. IN THE COMPILATION OF A USER DIRECTORY OR A DATABASE WE CAN FIND NO INTEREST COMPELLING ENOUGH TO WARRANT INFRINGEMENT OF THE RIGHTS OF USERS WHO DO NOT WISH TO PROVIDE THIS INFORMATION. THE MANDATORY DELIVERY TO THE AUTHORITIES OF SUCH

information, which could facilitate electronic surveillance, can only inhibit Tunisians wishing to express themselves or receive information online.

AIT's Contract Restricts Users' Rights. The contract presented to institutional clients by the AIT restricts their right to seek and access information online. The requirement that they use it only for "scientific, technological or commercial purposes that are strictly related to the activity of the client" apparently bars them from using the Internet account for personal or other business, under penalty of cancellation of the contract. The contract also violates the privacy of users by requiring that they inform the AIT of all persons who have access to their accounts.

In early 1999, the number of Tunisians online was estimated between 3,000 and 5,000. This figure seemed low for a middle-income country of seven million with a relatively high rate of educational attainment and a good phone system. There were, moreover, few Internet accounts at universities, which are all public institutions, and at nongovernmental organizations. These two sectors exhibit relatively high rates of Internet connectivity in many other middle-income countries.

Beginning in 1999, the government has taken measures to accelerate the growth of Internet use. Prices for Internet accounts dropped through 1999 and the first half of 1999. Consulted on May 17, 1999, the web site of Planet advertised a rate for households of about U.S. \$17 per month for unlimited usage during off-peak hours, a huge drop from two years earlier. In early 1999, articles in the local press forecast that, thanks to government initiatives, the number of users would reach 30,000 during 1999.

Human Rights Watch interviewed several Tunisians who concurred that the process of obtaining Internet access had grown more efficient and reliable since 1999. They said that prior to 1999, few Tunisians had access to the Internet and that applications were often delayed or simply never processed. These individuals, who are not outspoken dissidents and requested anonymity, all said they believed that police scrutiny of each application and government wariness toward allowing widespread Internet access explained these past delays in processing applications, the absence of Internet cafés until late 1999 (see below) and, more generally, the low number of users in the country.

According to the government, "access for individuals, organizations and companies to Internet services is made available simply by applying to the ISP of their choice." The applicant is not required to notify or obtain permission from any governmental entity. However, almost all of those we interviewed said they knew of persons who had applied for Internet services in past years and who had waited months for a response, or who received no response at all. They also said they had heard of persons whose accounts were terminated without explanation. A university professor told Human Rights Watch in October 1999 how his application was ignored: "Two years ago, I received mail, inviting me to apply for an Internet account. It

CONTAINED A COPY OF A CONTRACT, WHICH SAID I WOULD BE RESPONSIBLE FOR HOW THE ACCOUNT WAS USED, AND SAID I WOULD HAVE TO PLEDGE TO USE IT ONLY FOR PROFESSIONAL PURPOSES, AND SO ON. I FILLED IT OUT AND SENT IT IN, BUT NEVER RECEIVED ANY RESPONSE.”

A PROFESSOR AT THE LAW SCHOOL IN SOUSSE TOLD HUMAN RIGHTS WATCH IN AUGUST 1998 THAT FEW PROFESSORS IN TUNISIA HAVE INTERNET ACCOUNTS; HE SAID THAT HIS LAW FACULTY HAD NO INTERNET ACCOUNT. A PROFESSOR WHO TEACHES AT THE UNIVERSITY OF TUNIS TOLD HUMAN RIGHTS WATCH THAT SOME ACADEMIC DEPARTMENTS WERE GIVEN A SINGLE INTERNET ACCOUNT, WITH A WARNING TO THE SENIOR FACULTY MEMBER THAT HE OR SHE WAS RESPONSIBLE FOR ALL USE OF THE ACCOUNT. A SIMILAR WARNING WAS DELIVERED TO THE EXECUTIVE DIRECTOR OF ONE OF THE FEW NONGOVERNMENTAL ORGANIZATIONS TO ENJOY INTERNET ACCESS.

WITHOUT EXCEPTION, THE TUNISIANS WE INTERVIEWED SAID THEY BELIEVED THE GOVERNMENT MONITORED E-MAIL CORRESPONDENCE. NONE OF THEM COULD CITE CONCRETE EVIDENCE FOR THIS, BUT SAID THEY MADE THIS ASSUMPTION BECAUSE OF THE LEVEL OF POLICE SURVEILLANCE OF TELEPHONE CONVERSATIONS AND OTHER ASPECTS OF TUNISIAN LIFE,¹²⁵ AND INCIDENTS WHERE E-MAILS WERE LOST OR DELAYED BY ONE DAY OR LONGER WHILE EN ROUTE.

TUNISIA'S BLOCKING OF WEB SITES IS ANOTHER MANIFESTATION OF ITS VIGILANCE OVER THE FLOW OF INFORMATION ONLINE. THE GOVERNMENT, IN ITS LETTER TO HUMAN RIGHTS WATCH, AVOIDS ANY ALLUSION TO BLOCKING WEB SITES ON THE BASIS OF POLITICAL CONTENT AND SUGGESTS THAT ANY BLOCKING IS MOTIVATED BY MORAL AND PRIVACY CONCERNS:

TUNISIA IS COMMITTED TO THE PRINCIPLE OF PRESERVING MORAL VALUES AND THE PROTECTION OF PERSONAL PRIVACY. WEB SITES, ELECTRONIC COMMUNICATIONS, AND OTHER ONLINE FORUMS THAT DO NOT COMPLY WITH THESE PRINCIPLES (PEDOPHILIA, PORNOGRAPHY, ETC.) ARE IN VIOLATION OF THE LAW. TUNISIA IS FOLLOWING WITH INTEREST THE DEBATES OVER THIS QUESTION ON AN INTERNATIONAL SCALE, IN ORDER TO FIND APPROPRIATE SOLUTIONS.

¹²⁵ THE U.S. STATE DEPARTMENT'S *COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES* FOR 1998 REPORTED, "THERE WERE NUMEROUS REPORTS OF GOVERNMENT INTERCEPTION OF FACSIMILE AND COMPUTER-TRANSMITTED COMMUNICATIONS."

In fact, authorities also block some web sites containing information critical of Tunisia's human rights record. Internet users in Tunisia reported that they could not access the web sites of Amnesty International (<www.amnesty.org>) and the Committee To Protect Journalists (<www.cpj.org>), a New York-based group that in 1998 and 1999 cited President Ben Ali on a list of press freedom's ten greatest "enemies." One user said he believed that authorities had also blocked <www.mycable.org>, a web site that offered free web-page hosting and sometimes carried material on Tunisia (there were, for example, links to many human rights reports critical of Tunisia at <www.mycable.org/~maghreb>). Another user reported in late 1998 that the site <www.i-france.com/EFAl>, which contains the texts of Amnesty International reports in French, was also blocked. The web site of Reporters sans frontières (<www.rsf.fr>) was also blocked, according to the small independent Tunisian magazine *al-Manaqif*.¹²⁶

Absent a government confirmation, it is not always possible to confirm that a site is inaccessible due to blocking rather than to technical problems. However, in the case of the Amnesty International web site, at least, the evidence clearly points to intentional blocking.

¹²⁶ *Jāyeb Ma'li*, "Fukku al-Riqaba 'an al-Internet!" ("End Censorship of the Internet!") *al-Manaqif*, January 1999.

A private firm with friendly ties to the Tunisian government mounted a web site with a URL that appeared likely to fool persons trying to access Amnesty International information. The site, <www.amnesty-tunisia.org>, closely tracked the government's own rhetoric on human rights while avoiding any mention of Amnesty International. Tunisian authorities denied any role in the web site.¹²⁷ The domain name is registered to the Paris-based Euromed Group (<www.euromed.com>). Euromed chairman Rachid el-Chammah, who conducts business in Tunisia, insisted in a press interview that the web site was his own project and that he chose the word "amnesty" because it was appropriate for a human rights site and not because it was the name of a prominent organization critical of Tunisia's record on rights.¹²⁸ In a counter-offensive, Amnesty International launched a web site, <www.amnesty.org/tunisia>, that juxtaposed the pro-Tunisian positions found at <www.amnesty-tunisia.org> with its own assessment of the human rights situation.¹²⁹ The contents of <www.amnesty-tunisia.org> was subsequently withdrawn and replaced by a statement condemning Amnesty International's tactics as an effort "to show its new prowess in cyberpropaganda." The original contents were moved to a new site, <www.rights-tunisia.org>.

In late 1998, the first Internet cafés opened in Tunisia, long after they had proliferated in Morocco, Egypt, Jordan, and elsewhere. According to a European journalist who visited two of them in greater Tunis in February 1999, the "Publnet" cafés had certain local characteristics. First, in both locations, the monitors were all positioned so that their screens were visible to the administrator of the café, thus diminishing user privacy. Second, in one of the cafés, clients were asked to present identity documents, and in the other location they were asked their names and addresses. This requirement deprives users of their right to use the

¹²⁷ "Web: L'affirmation d'Amnesty est 'ridicule', selon l'ambassade de Tunisie," *Agence France-Presse*, November 27, 1999.

¹²⁸ Pamela Mendels, "Rights Group Fights a Foe with Frames," *New York Times CyberTimes* (online), February 16, 1999, <www.nytimes.com/library/tech/99/02/cyber/articles/16amnesty.html>. See also Roula Khalaf, "Amnesty Defends Itself," *Financial Times*, February 13, 1999.

¹²⁹ Amnesty International press release, February 1, 1999, ACT 93/01/99.

INTERNET ANONYMOUSLY AND IS APPARENTLY INTENDED TO ENSURE SOME OVERSIGHT OF INTERNET USE AT THESE NEW PUBLIC POINTS OF ACCESS.

United Arab Emirates

THE UNITED ARAB EMIRATES, ONE OF THE WORLD'S WEALTHIEST AND MOST TECHNOLOGICALLY MODERN COUNTRIES,¹⁰⁰ CAN ALSO CLAIM TO BEING THE MOST WIRED STATE IN THE ARAB WORLD. AS OF OCTOBER 1999 IT HAD 52,000 SUBSCRIBERS AND 143,000 USERS, ACCORDING TO ONE ESTIMATE.¹⁰¹ THE COUNTRY HAS NUMEROUS CYBERCAFÉS, AND, ACCORDING TO THE MIDDLE EAST INTERNET DIRECTORY FOR 1999, THE LARGEST NUMBER OF CORPORATE WEB SITES.¹⁰² GOVERNMENT MINISTRIES MAINTAIN SOPHISTICATED WEB SITES AND A PUBLIC-SECTOR THINK-TANK, THE EMIRATES CENTER FOR STRATEGIC STUDIES AND RESEARCH (<www.ecssr.ac.ae>), HOSTS INTERNATIONAL CONFERENCES ON THE INFORMATION REVOLUTION IN THE REGION.¹⁰³

THE U.A.E. HAS AT THE SAME TIME BEEN THE REGIONAL LEADER IN ADVOCATING CENSORSHIP OF THE WEB THROUGH THE USE OF HIGH-TECH MEANS. AN OFFICIAL WITH ETISALAT (THE EMIRATES TELECOMMUNICATIONS CORPORATION), WHICH IS THE COUNTRY'S STATE-CONTROLLED TELECOMMUNICATIONS MONOPOLY AND SOLE INTERNET PROVIDER, WAS QUOTED IN 1997 AS SAYING, "SINGAPORE HAS SUCCEEDED TO A GREAT EXTENT IN ITS DRIVE TO CONTROL HARM DONE BY THE INTERNET. WHY CANNOT WE?"¹⁰⁴

DIAL-UP USERS IN THE U.A.E. DO NOT ACCESS THE INTERNET DIRECTLY. THEY DIAL IN TO A PROXY SERVER MAINTAINED BY ETISALAT. THE PROXY WILL REFUSE ACCESS TO WEB SITES IF THE URL REQUESTED IS

¹⁰⁰ WORLD BANK, *WORLD DEVELOPMENT REPORT, 1998/99* (OXFORD: OXFORD UNIVERSITY PRESS, PUBLISHED FOR THE WORLD BANK, 1999), AND INTERNATIONAL TELECOMMUNICATION UNION, *WORLD TELECOMMUNICATION DEVELOPMENT REPORT, 3RD ED., 1996/97* (GENEVA: INTERNATIONAL TELECOMMUNICATION UNION, 1997). THE ITU WEB SITE, <www.itu.int>, HAS LINKS TO A VARIETY OF COUNTRY-BY-COUNTRY TELECOMMUNICATIONS STATISTICS.

¹⁰¹ SURVEY PUBLISHED IN THE NOVEMBER 1999 *INTERNET AL-ALAM AL-ARABI* MAGAZINE (<www.ianmag.com>), SUMMARIZED IN ENGLISH AT <www.ditnet.co.ae/me_internet.html>.

¹⁰² ALTHOUGH ONE ESTIMATE RANKED THE U.A.E. HIGHEST IN ABSOLUTE NUMBERS OF USERS, QATAR, WITH ITS SMALLER POPULATION, HAD A HIGHER PROPORTION OF ITS POPULATION USING THE INTERNET: 3.1 PERCENT AS OPPOSED TO 2.99 PERCENT IN JANUARY 1999. SEE APPENDIX A.

¹⁰³ IT SPONSORED, FOR EXAMPLE, "THE IMPACT OF THE INFORMATION AND COMMUNICATIONS REVOLUTION ON SOCIETY AND STATE IN THE ARAB WORLD," JANUARY 4-7, 1997. THE CONFERENCE PAPERS WERE PUBLISHED AS *THE INFORMATION REVOLUTION AND THE ARAB WORLD: ITS IMPACT ON STATE AND SOCIETY* (ABU DHABI: THE EMIRATES CENTER FOR STRATEGIC STUDIES AND RESEARCH, 1999).

¹⁰⁴ REUTERS, JANUARY 25, 1997.

ON A LIST OF BANNED SITES, OR IF A CONTENT CHECK OF THE SITE BY THE PROXY SERVER TURNS UP OBJECTIONABLE MATERIAL.

GOVERNMENT OFFICIALS, WHO ACKNOWLEDGED THAT THIS CENSORSHIP REGIME WAS ADMINISTERED BY THE STATE TELECOMMUNICATIONS COMPANY, INSISTED THAT ITS SOLE PURPOSE WAS TO BLOCK PORNOGRAPHIC SITES. A SENIOR OFFICIAL IN THE MINISTRY OF INFORMATION AND CULTURE, WHO WAS INTERVIEWED ON CONDITION HIS NAME NOT BE USED, TOLD HUMAN RIGHTS WATCH IN A TELEPHONE INTERVIEW ON JUNE 10, 1999:

THERE IS NO RESTRICTION ON THE POLITICAL, SOCIAL, ECONOMIC SIDE. POLITICALLY, IN THE U.A.E., WE DO NOT HOLD VALUE FOR CENSORSHIP, ESPECIALLY POLITICAL OR CENSORSHIP OF IDEAS: WE DON'T BELIEVE IN THAT. YOU CAN ACCESS ON THE INTERNET ANY MATERIAL, FROM ISRAEL OR ANYWHERE. THE WHOLE IDEA [OF THE PROXY SYSTEM] WAS TO BLOCK Y-RATED MATERIALS. YOU CAN SEE THE FIRST PAGES [OF SEXUALLY EXPLICIT SITES], BUT NOT WHATEVER IS AFTER THAT.

THE OFFICIAL ADDED THAT ALTHOUGH ETISALAT BLOCKS ATTEMPTS TO ACCESS PROSCRIBED MATERIAL, AUTHORITIES DO NOT TRACK INDIVIDUAL USERS' ONLINE ACTIVITIES. HOWEVER, SUCH MONITORING, IF IT EVER WERE TO BE CONDUCTED, WOULD BE FACILITATED BY THE FACT THAT ALL DIAL-IN USERS ARE CHANNLED THROUGH A PROXY SERVER OPERATED BY A PUBLIC UTILITY.

THE SAME OFFICIAL ACKNOWLEDGED THAT THE PROXY FILTERING SYSTEM WAS NOT FOOLPROOF. "YOU CAN GET TO PORNO," HE SAID, "BECAUSE YOU CAN ALWAYS JUST DIAL A FOREIGN SERVER. WE TRY OUR BEST TO LIMIT Y-RATED MATERIAL, BUT YOU CAN NEVER REALLY BUILD A WALL." OTHER OFFICIALS INTERVIEWED BY HUMAN RIGHTS WATCH CONCURRED AND ADDED THAT THE PROXY SERVER PREVENTS ACCESS ONLY FOR USERS WITH DIAL-UP SERVICE. USERS WHO CONNECT VIA A DEDICATED LINE—FOUND PRIMARILY IN WORKPLACES—ACCESS THE INTERNET DIRECTLY, BYPASSING THE CENSORSHIP IMPOSED BY THE PROXY SERVER.

AN OFFICIAL AT ETISALAT, WHO ALSO ASKED NOT TO BE NAMED, TOLD HUMAN RIGHTS WATCH IN A JUNE 10, 1999 TELEPHONE INTERVIEW THAT THE PROXY SYSTEM IS MAINTAINED IN COLLABORATION WITH A U.S. FIRM THAT IS CONTRACTED TO MAINTAIN AND UPDATE THE FILTERING SOFTWARE THAT IS RUN BY THE PROXY SERVER. THE ETISALAT STAFF REVIEWS WEB SITES, SOMETIMES RESPONDING TO COMPLAINTS OR TIPS FROM USERS, AND INFORMS THE U.S. COMPANY OF MATERIAL THEY WISH TO BLOCK. THE OFFICIAL REFUSED TO DISCLOSE THE NAME OF THE U.S. COMPANY, OR PROVIDE THE CRITERIA USED TO DETERMINE WHICH SITES ARE BLOCKED. ETISALAT PROVIDES THE U.S. COMPANY WITH "BROAD GUIDELINES," HE EXPLAINED, FOR ROOTING OUT OBJECTIONABLE SITES. DENYING THAT THIS INCLUDED POLITICAL OR CULTURAL SITES, HE SAID THE "GUIDELINES WE'VE PASSED ALONG ARE FAIRLY BASIC." THEY FOCUS ON THE "SEXUALLY EXPLICIT."

AN INFORMATION SYSTEMS MANAGER WHO WORKED FOR ETISALAT WHEN THE PROXY SERVER SYSTEM WAS BEING DEVELOPED IN THE MID-1990S TOLD HUMAN RIGHTS WATCH IN A JUNE 9, 1999 TELEPHONE INTERVIEW THAT THE SYSTEM WAS SET UP IN RESPONSE TO CONCERNS THAT "THERE WAS A GREAT DEAL OF MISUSE [OF THE INTERNET] AMONG TEENAGERS." TO COMPLEMENT THE FILTERING DONE BY THE U.S. COMPANY, ETISALAT "GOT A PROGRAM RUNNING WITH PARENTS, OR WITH WHOMEVER FINDS [AN

OBJECTIONABLE] SITE, SO THAT THE PERSON WILL INFORM ETISALAT AND THEN ETISALAT RESTRICTS IT. THERE'S A COMMITTEE OF TECHNICAL PEOPLE AT ETISALAT WHO LOOK AT THE SITE, AND VERIFY IT HAS NUDE PICTURES, AND THEN THEY STOP IT."

WHILE ALL OF THE EMIRATI OFFICIALS WE INTERVIEWED INSISTED THAT THE PROXY SERVER EXISTS ONLY TO BLOCK PORNOGRAPHY, HUMAN RIGHTS WATCH IDENTIFIED AT LEAST ONE BLOCKED SITE THAT IS CULTURAL AND POLITICAL IN NATURE. IT IS THE SITE OF THE GAY AND LESBIAN ARABIC SOCIETY (<www.glas.org>). WHEN ASKED ABOUT THE SITE, THE INFORMATION AND CULTURE MINISTRY OFFICIAL QUOTED ABOVE ACKNOWLEDGED THAT IT WAS BLOCKED, EXPLAINING, "WE GOT COMPLAINTS ABOUT IT."

GLAS DESCRIBES ITSELF IN ITS WEB SITE AS:

A NETWORKING ORGANIZATION FOR GAY AND LESBIANS OF ARAB DESCENT OR THOSE LIVING IN ARAB COUNTRIES. WE AIM TO PROMOTE POSITIVE IMAGES OF GAYS AND LESBIANS IN ARAB COMMUNITIES WORLDWIDE. WE ALSO PROVIDE A SUPPORT NETWORK FOR OUR MEMBERS WHILE FIGHTING FOR OUR HUMAN RIGHTS WHEREVER THEY ARE OPPRESSED. WE ARE PART OF THE GLOBAL GAY AND LESBIAN MOVEMENT SEEKING AN END TO INJUSTICE AND DISCRIMINATION BASED ON SEXUAL ORIENTATION.

THE GLAS WEB SITE HOSTS A CHAT-LINE, AND REPORTS AND EDITORIALIZES ON SUCH TOPICS AS AIDS, ASYLUM CASES INVOLVING GAYS AND TRANSSEXUALS, CIVIL MARRIAGES IN LEBANON, AND THE IMPRISONMENT OF POLITICAL DISSIDENTS IN THE REGION. IN MAY OF 1998, GLAS PROCLAIMED ON ITS WEB SITE:

WE ARE ALSO KEEPING TRACK OF FLAGRANT HUMAN RIGHTS VIOLATIONS IN GULF COUNTRIES AND PARTICULARLY IN THE U.A.E. WHERE RECENT DEPORTATION OF HIV PATIENTS HAS MADE HEADLINES....SUCH ACTIVITIES NEED TO BE DENOUNCED AT EVERY OCCASION. THE U.A.E. PUTS A LOT OF EFFORT AT PRESENTING ITSELF AS A MAJOR BUSINESS CENTER IN THE AREA. THE MESSAGE SHOULD BE SENT THAT HUMAN RIGHTS VIOLATIONS WILL NOT BE IGNORED AND THAT WE WILL MAKE SURE THEIR IMAGE CONTINUES TO BE TARNISHED AND THEIR VIOLATIONS DENOUNCED.

HUMAN RIGHTS WATCH IS UNAWARE OF WEB SITES BELONGING TO GOVERNMENTS OR POLITICAL MOVEMENTS THAT ARE BLOCKED IN THE U.A.E. HOWEVER, THE BLOCKING OF THE GLAS SITE INDICATES THAT INTERNET CENSORSHIP IN THE U.A.E. EXCEEDS THE PROCLAIMED GOAL OF RESTRICTING PORNOGRAPHY.

THE U.A.E. GOVERNMENT DID NOT REPLY IN WRITING TO THE LIST OF QUESTIONS SUBMITTED BY HUMAN RIGHTS WATCH TO ALL GOVERNMENTS OF THE REGION. IT DID HOWEVER INVITE HUMAN RIGHTS WATCH TO THE U.A.E. EMBASSY IN WASHINGTON TO DISCUSS INTERNET ISSUES. IN ADDITION, OFFICIALS IN THE MINISTRY OF INFORMATION AND CULTURE AND ANOTHER AT ETISALAT PROVED WILLING TO ANSWER SOME QUESTIONS DURING TELEPHONE INTERVIEWS WITH HUMAN RIGHTS WATCH; THEY ARE CITED ABOVE.

AT THE EMBASSY MEETING, HELD ON JULY 10, 1998, POLITICAL COUNSELOR ABDULLAH AL-SALEH AND LEGAL ADVISOR MOHAMED MATTAR EXPLAINED THAT INTERNET USERS ENJOYED CONSIDERABLE FREEDOM IN THE U.A.E., AND POINTED TO CONSTITUTIONAL GUARANTEES OF FREE EXPRESSION AND OF PRIVACY. ARTICLE 30

OF THE U.A.E. CONSTITUTION STATES, "FREEDOM OF OPINION AND EXPRESSING IT VERBALLY, IN WRITING OR BY OTHER MEANS OF EXPRESSION SHALL BE GUARANTEED WITHIN THE LIMITS OF LAW." ARTICLE 31 STATES, "FREEDOM OF COMMUNICATION BY POST, TELEGRAPH OR OTHER MEANS OF COMMUNICATION AND THE SECRECY THEREOF SHALL BE GUARANTEED IN ACCORDANCE WITH THE LAW." MATTAR SUGGESTED THAT THE REFERENCES IN THESE ARTICLES TO "OTHER MEANS" PRESUMABLY EXTENDED TO THE INTERNET. SIMILARLY, THE 1991 LAW ON TELECOMMUNICATIONS, WHICH AFFIRMS THE APPLICATION OF CRIMINAL LAW STATUTES (SUCH AS WITH RESPECT TO FRAUD) TO THE REALM OF TELECOMMUNICATIONS, WOULD APPLY TO CONDUCT ON THE INTERNET. HE STATED THAT THE U.A.E. HAD NO INTERNET-SPECIFIC LEGISLATION.

AL-SALEH ADDED THAT THE U.A.E.'S ONLY INTERVENTION WITH REGARD TO INTERNET USE CONCERNS THE BLOCKING OF WEB SITES. HE SAID THE STATE DOES NOT INTERFERE WITH OR CONDUCT SURVEILLANCE OF E-MAIL. THERE HAVE BEEN NO ARRESTS, HE SAID, OF PERSONS FOR ANY KIND OF "MISUSE" OF THE INTERNET. HUMAN RIGHTS WATCH HAS RECEIVED NO INFORMATION THAT CONTRADICTS HIS ASSERTIONS. HOWEVER, MAJ. GEN. DHAHI KHALFAN TAMIM, THE CHIEF OF POLICE OF DUBAI, ONE OF THE SEVEN CONSTITUENT EMIRATES OF THE U.A.E., PUBLICLY ADVOCATED POLICE OVERSIGHT OF THE INTERNET. IN 1996, FOR EXAMPLE, HE WAS QUOTED IN THE PRESS AS SAYING THAT THE MINISTRY OF INFORMATION AND THE POLICE, RATHER THAN ETISALAT, SHOULD BE RESPONSIBLE FOR LICENSING INTERNET USE. "IN ALL CASES, THE INFORMATION SHOULD BE FILTERED, SCANNED AND THEN MADE AVAILABLE TO USERS," THE GULF NEWS QUOTED HIM AS SAYING.¹⁵⁵ ASKED FOR COMMENT ON TAMIM'S PROPOSAL TO GIVE THE POLICE AND INFORMATION MINISTRY OVERSIGHT OF THE INTERNET, THE INFORMATION AND CULTURE MINISTRY OFFICIAL QUOTED ABOVE WROTE TO HUMAN RIGHTS WATCH ON JUNE 16, 1999 THAT THIS HAD NEVER BEEN IMPLEMENTED AND MERELY REPRESENTED "HIS [THE POLICE CHIEF'S] POINT OF VIEW."

THE SAME OFFICIAL ALSO STATED THAT ALL WEB SITES MUST BE REGISTERED WITH THE MINISTRY OF INFORMATION. "BUT THIS IS JUST A FORMALITY: WE'VE NEVER DENIED ANY REQUEST, AND DON'T THINK WE EVER WILL. WE DO NOT MONITOR THE MATERIAL. IT'S JUST TO MAKE SURE IT'S A REAL COMPANY," TO PREVENT COMMERCIAL FRAUD AND COPYRIGHT INFRINGEMENTS.

¹⁵⁵ "Dubai: Emirates Telecoms Group, Police in Internet Row," REUTERS, JUNE 19, 1996.

APPENDIX A
TABLE SHOWING INTERNET USE IN THE MIDDLE EAST

THE FOLLOWING TABLE AND ACCOMPANYING TEXT IS REPRINTED FROM THE WEB SITE OF NVA, LTD. (<www.nva.ie/surveys/how_many_online>), AN INFORMATION TECHNOLOGY COMPANY THAT PUBLISHES NUMEROUS SURVEYS OF INTERNET USE.

How Many Online?

THE ART OF ESTIMATING HOW MANY ARE ONLINE THROUGHOUT THE WORLD IS AN INEFFECTIVE ONE AT BEST. SURVEYS ABOUND, USING ALL SORTS OF MEASUREMENT PARAMETERS. HOWEVER, FROM OBSERVING MANY OF THE PUBLISHED SURVEYS OVER THE LAST TWO YEARS, HERE IS AN 'EDUCATED GUESS' AS TO HOW MANY ARE ONLINE WORLDWIDE AS OF MAY 1999. AND THE NUMBER IS 165 MILLION.

World Total 165 million
Africa: 1.14 million
Asia/Pacific: 26.97 million
Europe: 40.09 million
Middle East: 0.99 million
Canada & USA: 90.63 million
South America: 5.29 million

A NOTE ON SURVEY METHODOLOGY

- 'How Many Online' figures represent both adults and children who have accessed the Internet at least once during the 3 months prior to being surveyed.
- An Internet User represents a person with access to the Internet and is not specific to Internet Account holders. When the figure for Internet Account holders is the only information available, this figure is multiplied by a factor of 3 to give the number of Internet users.
- The figure for 'Asia/Pacific' includes Australia and New Zealand.
- When more than one survey is available on a country's demographics, NVA will take the mean of the two surveys or, in the case where NVA feels one study may be more comprehensive/reliable than the other, NVA will quote this figure over the other.

Middle East: How Many Online?

--	--	--	--

COUNTRY	DATE	NUMBER	% TOT POP.	SOURCE
U.A.E.	JANUARY 1998	89,552	2.99	DIT GROUP
U.A.E.	JULY 1997	45,150	1.47	DIT GROUP
Bahrain & Saudi Arabia	JANUARY 1998	46,538	0.23	DIT GROUP
Bahrain & Saudi Arabia	JULY 1997	38,480	0.19	DIT GROUP
ISRAEL	JANUARY 1999	600,000	10.8	IDC RESEARCH
ISRAEL	MAY 1998	300,000	5.5	INTERNET ISRAEL
JORDAN	JANUARY 1998	20,213	0.50	DIT GROUP
JORDAN	JULY 1997	11,840	0.28	DIT GROUP
Kuwait	JANUARY 1998	42,350	2.15	DIT GROUP
Kuwait	JULY 1997	29,600	1.51	DIT GROUP
LEBANON	JANUARY 1998	43,828	1.14	DIT GROUP
LEBANON	JULY 1997	35,520	0.95	DIT GROUP
OMAN	JANUARY 1998	20,888	0.95	DIT GROUP
OMAN	JULY 1997	11,425	0.52	DIT GROUP
QATAR	JANUARY 1998	17,295	3.10	DIT GROUP
QATAR	JULY 1997	8,265	1.51	DIT GROUP
YEMEN	DECEMBER 1997	2426	-	DIT GROUP

APPENDIX B: UNIFORM LETTER REQUESTING INFORMATION ON INTERNET POLICIES, SENT BY HUMAN RIGHTS WATCH IN MAY 1999 TO GOVERNMENTS OF THE REGION

APPENDIX C: REPLIES TO HUMAN RIGHTS WATCH LETTER RECEIVED FROM OFFICIALS OF IRAQ, JORDAN,
KUWAIT, QATAR, TUNISIA AND YEMEN

