Fordham International Law Journal

Volume 35, *Issue* 5 2017 *Article* 10

The Growth of Social Media Norms and the Governments' Attempts at Regulation

Alexandra Paslawsky*

*Fordham University School of Law

NOTE

THE GROWTH OF SOCIAL MEDIA NORMS AND GOVERNMENTS' ATTEMPTS AT REGULATION

Alexandra Paslawsky[*]

* J.D. Candidate, 2013, Fordham University School of Law; B.A., 2008, Boston College. The Author would like to thank Professor Olivier Sylvain for his encouragement and advice throughout the drafting process and her friends and family for their continual support. This Note received the William M. O'Connor Award for Student Work of the Year, 2011–2012.

> *"I think the time for censorship is gone . . . . Forces of technology, changing cultures, changing modes of communication . . . This is a phenomenon that no government or alliance of governments can block. This is evolution and no one can stop evolution."*[1]

INTRODUCTION

Ten years ago, the social media site Facebook did not exist.[2] YouTube and Twitter did not enter the cultural consciousness until 2005 and 2006, respectively.[3] These social media sites came into the world and subsequently transformed it by allowing people to connect with each other on an unprecedented level, free of charge.[4]

---

1. *Rumors of a Facebook Block Persist in Egypt*, MENASSAT, Aug. 29, 2008, http://www.menassat.com/?q=en/comment/reply/4508 (quoting Wael Nawara, Egyptian blogger).

2. *See Newsroom*, FACEBOOK, http://newsroom.fb.com/content/default.aspx?NewsAreaId=20 (last visited May 25, 2012) (tracing the history of Facebook).

3. *See* Nicholas Carlson, *How Twitter Was Founded*, BUS. INSIDER, Apr. 13, 2011, http://www.businessinsider.com/how-twitter-was-founded-2011-4 (discussing the founding of Twitter); John Cloud, *The YouTube Gurus*, TIME, Dec. 25, 2006, at 66 (presenting the history of YouTube).

4. *See* DAVID KIRKPATRICK, THE FACEBOOK EFFECT 7–8 (2010) (providing examples of how Facebook has changed the world); *see also infra* Part II (describing how people in different countries have used social media to effectuate change). While there are still costs to connecting to the Internet, such as connection fees, there is no charge to join social media sites such as Facebook and Twitter. *See* Carlson, *supra* note 3; *Newsroom*, *supra* note 2.

Social media sites have transformed society on both a micro and macro level by enabling perpetual communication.[5] On the micro level, individuals are able to keep track of their friends and family on a daily basis.[6] People can upload pictures, offer commentary on a topic of their choice, or voyeuristically view the activity of others.[7] With a single click, a person can receive updates on a friend who is on the other side of the world.[8] On the macro level, social media has enabled mass gatherings, helped to organized strikes, and facilitated revolutions around the world.[9]

No one could have predicted the way the Internet developed, spreading beyond borders to become an accepted (and expected) reality of everyday life.[10] Early commentators questioned how governments would respond to the spread of the Internet and whether an international approach to internet governance would develop.[11] The various laws of different

---

5. *See* Jan H. Kietzmann et al., *Social Media? Get Serious! Understanding the Functional Building Blocks of Social Media*, 54 BUS. HORIZONS 241, 241 (2011) (expounding the influence of social media in today's society); *see also* AARON SMITH ET AL., PEW INTERNET & AM. LIFE PROJECT, THE INTERNET AND CIVIL ENGAGEMENT 5–7 (2009), *available at* http://pewinternet.org/~/media//Files/Reports/2009/The%20Internet%20and%20Civic%20Engagement.pdf (positing that new forms of civic engagement through social media sites may alter long-standing patterns).

6. *See* Kietzmann et al., *supra* note 5, at 242 (discussing the ways that social media can be used); *see also Newsroom*, *supra* note 2 (providing information on the uses of Facebook).

7. *See* KIRKPATRICK, *supra* note 4, at 7–8 (discussing how people use Facebook); *see also* Kietzmann et al., *supra* note 5, at 242 (describing the ways individuals use social media).

8. *See* KIRKPATRICK, *supra* note 4, at 7–8 (providing examples of how social media has aided in organizing movements); *see also infra* Part II (describing how people in different countries have used social media to effectuate change).

9. *See infra* Part II (describing the role of social media in movements around the world).

10. *See, e.g.*, Steven M. Hanley, *International Internet Regulation: A Multinational Approach*, 16 MARSHALL J. COMPUTER & INFO. L. 997, 1012–13 (1998) (proposing an approach that would allow different countries to exercise varying degrees of regulation); Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT L. REV. 1257, 1260 (1998) (arguing that it would be unrealistic to expect that the rules of cyberspace could take over from existing laws); Timothy S. Wu, *Cyberspace Sovereignty?—The Internet and the International System*, 10 HARV. J.L. & TECH. 647, 658 (1997) (assuming that international governments would be able to shape internet norms and ignore those that did not benefit them).

11. *See* Hanley, *supra* note 10, at 1003–06 (presenting attempts at internet regulation); Lemley, *supra* note 10, at 1266–84 (describing the problems with enforcing

countries were seen as the major impediment towards establishing a comprehensive system of internet governance.[12] This assumed, however, that internet control would remain a viable option for governments.[13] While academics studying internet regulation noted its status quo-altering potential, none could predict how pervasive internet use (and dependence) would become.[14]

Over time, internet norms and rules were established and widely adopted, first by the engineering and technological groups responsible for initial internet development, and later by international organizations and governmental agencies.[15] Initially, internet experts pointed to different attitudes between "founding" countries (e.g., the United States) and countries that adopted the Internet later as a basis for why a governance framework that relied on internationally accepted principles and standards, such as transparency and privacy, would never emerge.[16] According to this view, the national agenda would always triumph if there were a clash between government

---

internet norms); Wu, *supra* note 10, at 648–49 (discussing the possible approaches to an international system of internet governance).

12. *See* Hanley, *supra* note 10, at 1010 ("Foreseeable problems arise in enforcing international laws enacted to regulate the Internet since countries hold vastly different political and social values."). *See generally* John T. Delacourt, *The International Impact of Internet Regulation*, 38 HARV. INT'L L.J. 207 (1997) (illustrating the different legal approaches taken by several countries in regulating the Internet).

13. *See* Hanley, *supra* note 10, at 1012–13 (discussing censorship as a possible governmental approach to internet regulation); *see also* Delacourt, *supra* note 12, at 208 (mentioning screening software and rating systems as ways that states could regulate the Internet).

14. *See* Amy Knoll, *Any Which Way but Loose: Nations Regulate the Internet*, 4 TUL. J. INT'L & COMP. L. 275, 299 (1996) ("[I]t appears that most of the authorities in many of the countries do not fully appreciate the global nature of the Internet."); *see also* Lemley, *supra* note 10, at 1267–71 (claiming that the establishment of a collective internet community would become impossible as the size of the group increases). *See generally* Hanley, *supra* note 10 (failing to predict how ubiquitous internet use would become).

15. *See infra* Part II (tracing the development of internet norms).

16. *See* Wu, *supra* note 10, at 661 ("The attitudes of 'founding' countries like the United States is profoundly different from that of countries for whom the Internet is a somewhat awkward recent arrival."); *see also* Hanley, *supra* note 10, at 1013–18 (stating that there is no international consensus and thus, "[o]ne rigid unitary solution to international Internet regulation is impossible"); *infra* Part I.B.2 (discussing the norms that have been adopted by international organizations).

interests and internet norms.[17] Consequently, a state would likely respect norms that promoted the long-term interests of the state and ignore the rest.[18] For example, a nation interested in regulating all content that reaches its citizens would ignore the accepted internet principles of freedom of expression and transparency.[19] Consequently, an international system of internet governance could never truly develop.[20]

Contrary to this early view, there is now de facto governance by international organizations, nongovernmental organizations ("NGOs"), corporations, and governmental agencies.[21] Historically, these groups have stressed privacy and freedom of expression as key norms that should influence any legislation that is adopted.[22] The Internet has enabled the dissemination of traditionally American notions of freedom of expression and privacy to regions unfamiliar with these ideas.[23] People around the world have embraced these democratic concepts and demanded change, and as a result, governments have had to

---

17. *See* Wu, *supra* note 10, at 665 ("[E]ven in the face of a strong individual consensus that a certain Internet norm deserves recognition by nation states, certain states may nonetheless refuse to adopt the norm."); *see also* Hanley, *supra* note 10, at 1001 ("Thus, governments of all Internet using countries are faced with a dilemma: how to allow the free exchange of information while at the same time prevent socially unacceptable information from entering their country via the Internet.").

18. *See* Wu, *supra* note 10, at 658 ("Those norms for which cooperation seems to facilitate the long-term interests of the state will become the governing rule set of the regime, while all others will simply be ignored."); *see also* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1390 (1996) (predicting that territorial sovereigns would continue to assert jurisdiction and make law about what happens online).

19. *See* Wu, *supra* note 10, at 659–60 (naming Singapore as an example of a nation that has ignored established internet norms in the interest of protecting its national interests); *see also* Johnson & Post, *supra* note 18, at 1381–87 (discussing how sovereigns continue to assert control over the Internet).

20. *See* Hanley, *supra* note 10, at 1016 ("One rigid unitary solution to international Internet regulation is impossible."); *see also* Wu, *supra* note 10, at 658–66 (describing why an international system of internet governance could never succeed).

21. *See infra* Part II (explaining the power these groups have in guiding the Internet's development and, consequently, in the way people view content); *see also* Christopher S. Yoo, *Free Speech and the Myth of the Internet as an Unintermediated Experience*, 78 GEO. WASH. L. REV. 697, 698–99 (2010) (describing the ways in which different groups act as intermediaries in order to facilitate the internet experience).

22. *See infra* Parts II–III (discussing the way in which internet norms emerged).

23. *See infra* Part II.A (recognizing that social media has allowed traditionally Western ideals to spread to other regions such as Middle East).

reassess their approach to internet regulation.[24] The rise of social media has shown that the Internet is truly a democratic medium, and international governments have struggled to respond to its continued growth and relevance.[25] Never before has a generation been so tech-savvy.[26] Governments, however, have not yet determined their proper role in this new system.[27]

Nations that experience a clash between the traditional norms of the state and accepted internet norms have had a more difficult time than those with similar principles.[28] For example, Egypt does not have traditional notions of free speech or privacy, and consequently, it was difficult for the state to respond when Egyptians expected that these norms would be respected on the Internet.[29] Even so, more technologically advanced countries such as the United Kingdom and the United States also have experienced growing pains.[30] This Note argues that going forward, governments should use established internet norms and standards when making important legislation and regulations. Rather than attempt to create an internet policy based solely on the existing sovereign laws, which do not account for technological realities, nations should aim to model future legislation within their countries on existing internet norms such as freedom of expression, transparency, and privacy.

Part I of this Note provides an overview of the Internet and social media. Specifically, it examines how norms were established as the Internet's cultural pervasiveness soared. Part I.A discusses the development of the Internet, using the United States, the United Kingdom, and Egypt as case studies. Next,

---

24. *See infra* Part II (identifying the problems governments have faced in trying to control the Internet).

25. *See infra* Part II (describing the issues that international governments have faced as social media has grown).

26. *See* Kietzmann et al., *supra* note 5, at 242 (describing the current state of technology and its influence on society); *see also* KIRKPATRICK, *supra* note 4, at 6–8 (naming ways in which people are able to use social media).

27. *See infra* Part II (identifying the problems governments have faced when attempting to regulate the Internet).

28. *See, e.g.*, *infra* Part II.A (describing the Egyptian government's response to the expectation that internet norms will be respected).

29. *See infra* Part II.A (discussing the difficulties the Egyptian government has faced as social media sites have become ubiquitous).

30. *See infra* Part II.B–C (setting forth the issues that the United Kingdom and the United States face when attempting to regulate social media).

Part I.B looks at how international organizations, engineering groups, and governmental agencies have adopted particular internet norms and standards. In particular, this Part looks at freedom of expression and privacy as norms that have historically guided regulation of the Internet. Part I.B also analyzes how governments have attempted to establish security as a norm in order to rationalize state interference with social media.

Part II then examines the governmental responses to social media sites such as Facebook and Twitter in Egypt, the United Kingdom, and the United States, and the recent clashes between these governments and established internet norms. Specifically, Part II.A traces the Egyptian revolution of early 2011. Part II.B discusses the UK riots of August 2011 and the recent development of the "super-injunction," an injunction that prevents news organizations from revealing the identities of those involved in legal disputes or even reporting the fact that restrictions have been imposed.[31] Finally, Part II.C looks at the repercussions of San Francisco's shutdown of mobile service in August 2011. Part II.C also examines the legal issues concerning the collection and storage of personal data by authorities in the United States and recent attempts to further restrict freedom of expression on the Internet.

In Part III, this Note argues that governments must respect established internet norms such as freedom of expression and privacy when attempting to regulate social media. Governmental use of a security rationale is not persuasive, as freedom of speech and privacy considerations have consistently trumped security concerns since the dawn of the Internet, especially in the American context. While the rise of social media may have amplified security concerns, the US government should remain true to its initial aspirations when formulating policy. This Note concludes that rather than taking steps to regulate social media as security threats arise, governments should instead look to internet norms such as openness, transparency, access, freedom

31. *See* James Robinson, *How Super-Injunctions Are Used to Gag Investigative Reporting*, GUARDIAN (U.K.), Oct. 13, 2009, at 6 (describing the creation of super-injunctions); Ravi Somaiya, *British Law Used to Shush Scandal Has Become One*, N.Y. TIMES, Apr. 27, 2011, at A4 (summarizing the elements of a super-injunction).

of expression, and privacy when determining social media policy.

I. *THE GROWTH OF THE INTERNET AND THE DEVELOPMENT OF NORMS AS A MEANS OF INTERNET GOVERNANCE*

The development of the Internet resulted in the emergence of standards and norms relating to internet governance.[32] These standards and norms were subsequently adopted internationally.[33] In order to understand how these norms emerged, it is first necessary to examine the evolution of the Internet. This Part traces the growth of the Internet and the competing technological norms that were adopted and implemented by governing organizations. Part I.A discusses the evolution of the Internet. Specifically, Part I.A examines the initial development of the Internet and attempts at regulation in the United States. Next, it tracks the growth of the Internet in other developed countries, such as the United Kingdom. Finally, Part I.A describes the spread of the Internet to the rest of the world, using Egypt as an example.

Next, Part I.B discusses how international organizations, engineering groups, and governmental agencies have adopted norms and standards. Specifically, this Part describes how freedom of expression and privacy are norms that have historically guided internet regulation. Part I.B also analyzes

---

32. *See, e.g.*, ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html [hereinafter OECD] (listing basic principles of data protection); INTERNET SOC'Y, EUROPEAN COMMISSION: PUBLIC CONSULTATION ON THE OPEN INTERNET AND NET NEUTRALITY (2010), *available at* http://www.isoc.org/pubpolpillar/docs/20100929_eu.pdf (describing the norms of openness and transparency as vital internet standards).

33. *See* Letter from Sally Shipman Wentworth, Reg'l Manager, N. Am., Internet Soc'y, to the Hon. Julius Genachowksi, Chairman, Fed. Commc'ns Comm'n (Jan. 14, 2010), *available at* http://www.isoc.org/pubpolpillar/docs/fcc_20100114.pdf (using internet norms and standards to validate preservation of the open Internet); *see also* World Summit on the Information Society, Geneva 2003–Tunis 2005, *Rep. from the Working Group on Internet Governance*, ¶¶ 6–7, WSIS-II/PC-3/DOC/5-E (Aug. 3, 2005) (recommending the adoption of accepted internet norms and standards when trying to establish a system of internet governance).

how international governments have begun to use security concerns as a rationale for interfering with social media.

A. *The Development and Expansion of the Internet*

1. The Invention of the Internet: The United States

In the 1960s and 1970s, the US Department of Defense Advanced Research Projects Agency ("ARPA") designed an experimental computer network called ARPAnet.[34] This network linked computers at universities and research institutions in the United States and in several countries that were members of the North Atlantic Treaty Organization ("NATO").[35] In the 1980s, the US Department of Defense adopted the Transmission Control Protocol/Internet Protocol as ARPAnet's system of digital message formats and rules.[36] The TCP/IP protocol was a key architectural construct that introduced gateways to handle disparities between networks and allowed for reliable communications between them.[37] The Internet Engineering Task Force was called upon to refine and extend these protocols and continues to do so today.[38] In the early 1990s, Congress

---

34. *See* ROBERT E. KAHN & VINTON G. CERF, WHAT IS THE INTERNET (AND WHAT MAKES IT WORK)? (1999), *reprinted in* OPEN ARCHITECTURE AS COMMUNICATIONS POLICY 17, 21 (Mark N. Cooper ed., 2004) (discussing the creation of ARPAnet); *see also* Knoll, *supra* note 14, at 276 ("In 1969 the United States Department of Defense (DoD) designed an experimental computer network, the ARPAnet."). The Advanced Research Projects Agency ("ARPA") is an agency responsible for the development of new technology for use by the military. *Our Work*, DEF. ADVANCED RES. PROJECTS AGENCY, http://www.darpa.mil/our_work/ (last visited May 25, 2012).

35. *See* KAHN & CERF, *supra* note 34, at 21 (describing the way ARPAnet worked); *see also* Knoll, *supra* note 14, at 276 ("Gradually, universities throughout the United States were linked to this web of computers, mostly in the math and sciences departments.").

36. *See* KAHN & CERF, *supra* note 34, at 23 (discussing the establishment of the TCP/IP protocol); *see also* CHARLES L. HEDRICK, RUTGERS UNIV., INTRODUCTION TO THE INTERNET PROTOCOLS (1987), *available at* http://www.uic.edu/depts/accc/network/ftp/v452.html (presenting an introduction to the TCP/IP protocol suite).

37. *See* KAHN & CERF, *supra* note 34, at 23 (discussing the adoption of the TCP/IP protocol suite); *see also* ED KROL, THE HITCHHIKER'S GUIDE TO THE INTERNET 2 (1987) ("As local area networks became more pervasive, many hosts became gateways to local networks. A network layer to allow the interoperation of these networks was developed and called Internet Protocol (IP).").

38. *See* KAHN & CERF, *supra* note 34, at 24 (stating the responsibilities of the Internet Engineering Task Force); *see also* Olivier Sylvain, *Internet Governance and Democratic Legitimacy*, 62 FED. COMM. L.J. 205, 212 (2010) (describing the Internet

passed the Scientific and Advanced Technology Act of 1992, legislation that allowed organizations to connect to the Internet to conduct commercial activities.[39] This allowed for the privatization of the Internet and resulted in its extensive development.[40]

While the strong protections of the US Constitution and the Bill of Rights have resulted in very little government-mandated filtering or censorship, the Internet became highly regulated as it expanded and developed in the United States.[41] Government agencies such as the Federal Trade Commission ("FTC") and the Federal Communications Commission ("FCC") were tasked with regulating certain areas of the Internet.[42] There continues to be debate over content regulation on the Internet concerning a wide range of topics such as gambling, cyber security, and dangers to children.[43] Many of the

---

Engineering Task Force ("IETF") as "the preeminent technical standard-setting organization for the industry").

39. *See* Scientific and Advanced Technology Act of 1992, 42 U.S.C. § 1862(g) (2006); *see also* KAHN & CERF, *supra* note 36, at 26 (describing legislation allowing for commercial activity on the Internet).

40. *See* KAHN & CERF, *supra* note 34, at 26 (mentioning the consequences of legislation allowing commercial activity on the Internet); *see also* Jay P. Kesan & Rajiv C. Shah, *Fool Us Once Shame on You—Fool Us Twice Shame on Us: What We Can Learn from the Privatizations of the Internet Backbone Network and the Domain Name System*, 79 WASH. U. L.Q. 89, 111–14 (2001) (discussing the privatization of the Internet).

41. *See* John Soma et al., *Bit-Wise but Privacy Foolish: Smarter E-Messaging Technologies Call for a Return to Core Privacy Principles*, 20 ALB. L.J. SCI. & TECH. 487, 491 (2010) (explaining how different agencies regulate internet communications issues); *see also* Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, *in* OPEN ARCHITECTURE AS COMMUNICATIONS POLICY, *supra* note 34, at 41, 42 (describing internet regulation).

42. *See* Soma et al., *supra* note 41, at 491 (stating that both the Federal Communications Commission ("FCC") and Federal Trade Commission ("FTC") regulate internet and online communications issues); *see also* Lemley & Lessig, *supra* note 41, at 42 (discussing the duties of the FCC and FTC). The FCC regulates interstate and international communications by radio, television, wire, satellite, and cable in all fifty states, the District of Columbia, and US territories. *See What We Do*, FED. COMM. COMMISSION, http://www.fcc.gov/what-we-do (last visited May 25, 2012). The FTC's mission is to prevent business practices that are anticompetitive, deceptive, or unfair to consumers and to enhance informed consumer choice and public understanding of the competitive process without unduly burdening legitimate business activity. *About the Federal Trade Commission*, FED. TRADE COMMISSION, http://www.ftc.gov/ftc/about.shtm (last visited May 25, 2012).

43. *See United States and Canada Overview*, OPENNET INITIATIVE, 370, http://opennet.net/sites/opennet.net/files/ONI_UnitedStatesandCanada_2010.pdf (last visited May 25, 2012) (describing the areas where there continues to be debate

ongoing issues concern the First and Fourth Amendments of the US Constitution.

The First Amendment states: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."[44] In essence, the US government has no power to restrict expression because of its message, ideas, subject matter, or content.[45] Nevertheless, the protections of the First Amendment are not absolute.[46] The US Supreme Court has often recognized that reasonable time, place, and manner regulations may be necessary to further significant governmental interests.[47] These restrictions may be valid so long as they are not based on the content or subject matter of the regulated speech, serve a significant governmental interest, and "leave open ample alternative channels of communication."[48]

On the other hand, according to US law, restrictions that are content-based must be narrowly tailored and serve a

---

over the proper role of government in internet regulation); *see also* Danielle Keats Citron & Helen Norton, *Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age*, 91 B.U. L. REV. 1435, 1438–40 (2011) (exploring different ways to regulate content on the Internet).

44. U.S. CONST. amend. I.

45. *See* Police Dep't v. Mosley, 408 U.S. 92, 95 (1972) (holding that a city ordinance prohibiting all picketing within 150 feet of a school, except peaceful picketing of any school involved in a labor dispute, was unconstitutional because it made an impermissible distinction between peaceful labor picketing and other peaceful picketing, thereby restricting expression based on its message).

46. *See id.* at 98 (recognizing that reasonable time, place, and manner regulations of picketing may be necessary to further significant governmental interests).

47. *See, e.g.*, *id.* at 98; Heffron v. Int'l Soc'y for Krishna Consciousness, Inc., 452 U.S. 640, 645–46 (1981) (holding that a state's interest in maintaining orderly movement of crowd at a fair was sufficient to justify requirements); Grayned v. City of Rockford, 408 U.S. 104, 119 (1972) (allowing an antinoise ordinance aimed at preventing interference with nearby schools); Cox v. New Hampshire, 312 U.S. 569, 576 (1941) (finding a permit that fixed the time and place of a parade permissible because it served to prevent confusion by overlapping parades or processions, to secure convenient use of the streets by other travelers, and to minimize the risk of disorder).

48. *Heffron*, 452 U.S. at 647–48 ("We have often approved restrictions of that kind provided that they are justified without reference to the content of the regulated speech, that they serve a significant governmental interest, and that in doing so they leave open ample alternative channels for communication of the information.").

compelling state interest.[49] Consequently, many government-mandated attempts to regulate content have been banned on First Amendment grounds, often after lengthy legal battles.[50] The first wave of regulatory actions against sexually explicit material on the Internet came in the 1990s.[51] The Communications Decency Act of 1996 ("CDA"), for example, was designed to criminalize the transmission and display of patently offensive content and communications to minors.[52] This law was repealed in parts by the US Supreme Court in *Reno v. ACLU* because it was not narrowly tailored.[53]

Other sections of the CDA continue to remain in force, including Section 230, which grants internet service providers ("ISPs") immunity from liability arising from content that users place online and from requirements to remove offensive speech.[54] The First Amendment protects speech only from governmental restriction and thus does not govern private actors' decisions to remove or filter online expression.[55]

---

49. *Id.* at 662–63 (holding that the restriction was not narrowly drawn to advance the state's interests and therefore was unconstitutional).

50. *See* Reno v. ACLU, 521 U.S. 844 (1997) (striking down parts of the Communications Decency Act ("CDA") for violating the free speech provision of the First Amendment); *see also United States and Canada Overview*, *supra* note 43 (discussing *Reno*, 521 U.S. at 844, and its aftermath).

51. *See, e.g.*, Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 133 (codified as amended at 47 U.S.C. § 223 (2006)); *see also United States and Canada Overview*, *supra* note 43 (providing background on regulatory action taken in the United States).

52. 47 U.S.C. § 223; *see also United States and Canada Overview*, *supra* note 43 (discussing the CDA).

53. *Reno*, 521 U.S. at 846. Congress has made two narrower attempts to regulate children's exposure to internet indecency since the Supreme Court overturned parts of the Communications Decency Act ("CDA"). The US Supreme Court overturned the first, the Child Online Protection Act, for being vague and not narrowly tailored. *See* Ashcroft v. ACLU, 535 U.S. 564, 585–86 (2004). While legal challenges also followed the Child Online Protection Act's successor, the Children's Internet Protection Act of 2000, the Supreme Court upheld it as constitutional. *See* United States v. Am. Library Ass'n, Inc., 539 U.S. 194, 214 (2003).

54. 47 U.S.C. § 230; *see* Citron & Norton, *supra* note 43, at 1453 (analyzing the importance of Section 230 of the CDA).

55. *See* Langdon v. Google, Inc., 474 F. Supp. 2d 622, 631 (D. Del. 2007); *see also* Citron & Norton, *supra* note 43, at 1453 (explaining how private actors have the power to filter online expression).

Intermediaries therefore enjoy wide latitude to make many decisions regarding content.[56]

Regulation of the Internet also has raised Fourth Amendment concerns.[57] The Fourth Amendment of the US Constitution states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[58]

As technological advancements have created new legal concerns, the Fourth Amendment has become a source of challenges to existing legislation.[59]

The Electronic Communications Privacy Act ("ECPA"), as enacted into law, governs electronic communications, including e-mail and other types of electronic messaging.[60] Congress enacted the ECPA in 1986 to extend government restrictions on wiretaps from telephone calls to include transmissions of electronic data by a computer.[61] The ECPA also contains the Stored Communications Act ("SCA"), which addresses

---

56. *See* Citron & Norton, *supra* note 43, at 1453–54 (discussing the importance of CDA Section 230 in allowing private actors to regulate online expression); Yoo, *supra* note 21, at 697–702 (expounding ways in which intermediaries make decisions regarding internet content).

57. *See, e.g.*, Julia Angwin, *Secret Orders Target Email: Wikileaks Backer's Information Sought*, WALL ST. J., Oct. 10, 2011, at A1 (describing secret court orders made by the US government for personal information); Miguel Helft & Claire Cain Miller, *Web Outruns Privacy Law*, N.Y. TIMES, Jan. 10, 2011, at A1 (addressing Fourth Amendment concerns regarding the Electronic Communications Privacy Act ("ECPA")).

58. U.S. CONST. amend. IV.

59. *See, e.g.*, United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (addressing individuals' right to privacy in e-mail); *see also* David Kravets, *Justice Dept. to Congress: Don't Saddle 4th Amendment on Us*, WIRED (Apr. 7, 2011, 4:06 PM), http://www.wired.com/threatlevel/2011/04/fourth-amendment-e-mail-2/ (discussing the privacy issues of the ECPA).

60. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

61. *Electronic Communications Privacy Act: Hearings Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. of the Judiciary on H.R. 3378*, 99th Cong. 3 (1986) (statement of Sen. Patrick A. Leahy) (explaining the reasons for enacting the ECPA).

disclosure of stored communications held by third-party ISPs.[62] There are questions as to whether the ECPA (and more specifically, the SCA) violates the Fourth Amendment protections against unreasonable search and seizures.[63]

According to the ECPA, government officials do not need a warrant to read e-mail messages that are older than 180 days.[64] At the time the law was enacted, most e-mail was stored on a person's hard drive, and e-mail stored on a third-party server for more than six months was considered abandoned.[65] Recent technological developments (most notably, the practice of storing e-mail in the "cloud" rather than on a person's hard drive) have led many to believe the law is severely outdated and in need of revision.[66]

The ECPA also allows the government to compel disclosure of electronic records help by third-party ISPs.[67] Effectively, this provision allows government agents to monitor electronic communications systems for various reasons without a warrant.[68] For example, the US government has issued orders forcing Google and several other ISPs to turn over information from e-mail accounts.[69] Law enforcement regularly analyzes

---

62. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, §§ 201–202, 100 Stat. 1848, 1860 (codified at 18 U.S.C. §§ 2701–2712 (2006)).

63. *See* Helft & Miller, *supra* note 57, at A1 (discussing the problems that have resulted as the ECPA has become outdated); *see also* Kravets, *supra* note 59 (addressing the privacy issues of the ECPA).

64. 18 U.S.C. § 2703(a) (2006).

65. *See* Kravets, *supra* note 59 (comparing the current technological realities with those at the time the bill was signed into law); J. BECKWITH BURR, THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986: PRINCIPLES FOR REFORM 7–8 (2010), *available at* http://digitalduceprocess.org/files/DDP_Burr_Memo.pdf (criticizing the 180 day distinction).

66. *See* Helft & Miller, *supra* note 57, at A1 (discussing the need for new regulations that would clarify the law concerning legal wiretaps of various internet communications); *see also* Kravets, *supra* note 59 ("A coalition of internet service providers and other groups . . . has lobbied for an update to the law to treat both cloud- and home-stored e-mail the same, and thus require a probable-cause warrant for access.").

67. 18 U.S.C. § 2510(5) (2006).

68. *Id.*; *see* Soma et al., *supra* note 41, at 519–21 (analyzing the consequences of the ECPA).

69. *See* Angwin, *supra* note 57, at A1 (detailing a secret court order made by the US government); Noam Cohen, *Twitter Shines a Spotlight on Secret F.B.I. Subpoenas*, N.Y. TIMES, Jan. 10, 2011, at B3 (discussing how government subpoenas for information are often kept secret from the people being investigated).

information available on social networks to identify criminals, terrorists, and other threats.[70]

Courts have split on whether a person has a reasonable expectation of privacy in his or her e-mail.[71] Most recently, in 2010, the Sixth Circuit ruled in *United States v. Warshak* that a person has a reasonable expectation of privacy in his e-mails and that the government violated the Fourth Amendment by compelling an ISP to turn over e-mails without first obtaining a warrant.[72] The court went so far to say that the SCA was unconstitutional to the extent that it "purport[ed] to permit the government to obtain such e-mails warrantlessly."[73] The trend appears to be towards giving e-mail content the same privacy protections as postal mail or telephone conversations.[74]

Critics maintain that the ECPA should be changed to reflect technological realities.[75] Increasingly, courts have been moving to extend Fourth Amendment protection to electronic communications, and it appears that the US Congress is

---

70. *See* Danielle Keats Citron, *Fulfilling Government 2.0's Promise with Robust Privacy Protections*, 78 GEO. WASH. L. REV. 822, 831 (2010) (explicating how the government uses individuals' social-media information); *see also, e.g.*, Angwin, *supra* note 57, at A1 (discussing a secret court order obtained by the US government against a man who volunteered for Wikileaks, the website that released classified government diplomatic cables in 2011); Jim McKay, *Cops on the Tweet to Solve Crimes and Educate the Public*, PUB. CIO (Aug. 31, 2009), http://www.govtech.com/pcio/Cops-on-the-Tweet-to-Solve.html ("Now there's an almost constant police presence on these sites: behind the scenes where they may be quietly hunting sex offenders, or an upfront approach by posting videos and evidence to elicit public response that might help solve a crime.").

71. *See* Rehberg v. Paulk, 598 F.3d 1268, 1281 (11th Cir. 2010) (finding that a person does not have a reasonable expectation of privacy in an e-mail once any copy of the communication is delivered to a third-party); United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008) (holding that the privacy interests in e-mail are identical to those in postal mail and that message contents in both may deserve Fourth Amendment protection).

72. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

73. *Id.* at 288.

74. *See, e.g.*, *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827 (S.D. Tex. 2010) (ruling that the government must have a warrant when making requests for records from cellular services); ACLU v. Nat'l Sec. Agency, 438 F. Supp. 2d 754 (E.D. Mich. 2006), *rev'd and vacated on other grounds*, 493 F.3d 644 (6th Cir. 2007), *cert. denied*, 128 S. Ct. 1334 (2008) (holding that the Terrorist Surveillance Program, a foreign intelligence program that intercepted international telephone and internet communications without a warrant, was unconstitutional). *But see* United States v. Graham, CRIM. No. RDB-11-0094, 2012 WL 691531 (D. Md. Mar. 1, 2012).

75. *See* Helft & Miller, *supra* note 57, at A1 (criticizing the ECPA); Kravets, *supra* note 59 (noting the problems with the ECPA).

adopting a similar view.[76] The ECPA Amendments Act, a pending bill sponsored by chairman of the Senate Judiciary Committee, Senator Patrick Leahy (D-Vermont) would contain enhanced privacy protections, including a requirement that the government obtain a search warrant for all electronic content.[77]

2. The Spread of the Internet: The United Kingdom

As internet use became more common around the world, the debates in the United States over regulation and privacy spread to other countries like the United Kingdom. As a NATO member, the United Kingdom participated in the initial establishment of ARPAnet.[78] Although the United Kingdom is a constitutional monarchy without a written constitution, there is legal protection for the freedom of expression, the protection of reputation, and the right to privacy.[79] Additionally, the United Kingdom's Human Rights Act of 1998 provides for limited incorporation of the European Convention on Human Rights

---

76. *See* Press Release, Sen. Patrick Leahy, Leahy Introduces Benchmark Bill to Update Key Digital Privacy Law (May 17, 2011), *available at* http://leahy.senate.gov/press/press_releases/release/?id=b6d1f687-f2f7-48a4-80bc-29c3c5f758f2 ("Updating this law to reflect the realities of our time is essential to ensuring that our federal privacy laws keep pace with new technologies and the new threats to our security."); *see also* Liz Klimas, *Does 25-Year-Old Legislation Adequately Protect Internet Privacy?*, BLAZE (Oct. 21, 2011, 11:30 PM), http://www.theblaze.com/stories/does-25-year-old-legislation-adequately-protect-internet-privacy/ (discussing Senator Leahy's proposal to update the law).

77. *See* Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011); Klimas, *supra* note 76 (discussing Senator Leahy's proposed privacy protections); Press Release, Sen. Patrick Leahy, *supra* note 76 (outlining the proposal to overhaul the ECPA).

78. *See* KAHN & CERF, *supra* note 34, at 21 (explaining how the ARPAnet network was linked to computers at several British universities); Barry M. Leiner et al., *A Brief History of the Internet*, INTERNET SOC'Y, http://www.internetsociety.org/internet/internet-51/history-internet/brief-history-internet (last visited May 25, 2012) (discussing the role played by the United Kingdom in the establishment of the network).

79. *See* Campbell v. MGN Ltd., [2004] UKHL 22, [2004] 2 A.C. (H.L.) 457 (appeal taken from Eng.) (protecting a celebrity's privacy); Reynolds v. Times Newspapers Ltd., [1999] UKHL 45, [2001] 2 A.C. (H.L.) 127 (appeal taken from Eng.) (stressing the social importance of protecting reputation); James v. Commonwealth, [1936] A.C. 578 (P.C.) (appeal taken from High Court of Australia) (expounding the negative right of free speech present in English law); *Overview of the UK System of Government*, DIRECTGOV, http://www.direct.gov.uk/en/governmentcitizensandrights/ukgovernment/centralgovernmentandthemonarchy/dg_073438 (last visited May 25, 2012) (presenting an overview of the UK government).

into domestic law, which includes the right to privacy and freedom of expression.[80]

Specifically, Article 8 of the European Convention on Human Rights provides that "[e]veryone has the right to respect for his private and family life, his home and his correspondence."[81] Article 10 states: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."[82]

The United Kingdom's understanding of freedom of speech is very different than the understanding in the United States.[83] While the US Constitution weighs heavily in favor of protecting the freedom of expression, the United Kingdom has a very strong libel regime that seeks to protect the right to reputation and privacy.[84] As a result, free speech considerations are not as highly valued.[85] One example of this trend is the recent development of the super-injunction.[86] Relying on the right to privacy contained in the European Convention of Human Rights, UK courts have begun issuing injunctions that prevent news organizations from revealing the identities of those

---

80. Human Rights Act, 1998, c. 42 (Eng.); Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 222 [hereinafter ECHR].

81. ECHR, *supra* note 80, art. 8, 213 U.N.T.S. at 230.

82. *Id.* art. 10, 213 U.N.T.S. at 230.

83. *See* FREDERICK W. MAITLAND & FRANCIS C. MONTAGUE, A SKETCH OF ENGLISH LEGAL HISTORY 161 (James F. Colby ed., 1998) (introducing the development of law in the United Kingdom); *see also* ALASTAIR MULLIS & ANDREW SCOTT, SOMETHING ROTTEN IN THE STATE OF ENGLISH LIBEL LAW?: A REJOINDER TO THE CLAMOUR FOR REFORM OF DEFEMATION ¶ 17 (2010) (stating that "[t]here are observable differences when comparing the law of England and Wales with that of the United States").

84. *Compare Reynolds*, [1999] UKHL 45 (affirming that "reputation is an integral and important part of the dignity of the individual" and then went further to state that "protection of reputation is conducive to the public good"), *with* Citizens United v. FEC, 130 S. Ct. 876, 891 (2010) ("First Amendment standards, however, 'must give the benefit of any doubt to protecting rather than stifling speech.'").

85. *See, e.g.*, MULLIS & SCOTT, *supra* note 83, ¶¶ 9–11 (discussing attempts at reforming the libel regime in the United Kingdom); Robinson, *supra* note 31, at 6 (describing the creation of super-injunctions).

86. *See* Robinson, *supra* note 31, at 6 (providing a definition of a super-injunction); *see also* Somaiya, *supra* note 31, at A4 (summarizing the elements of a super-injunction).

involved in legal disputes, or even reporting the fact that restrictions have been imposed.[87]

These kinds of developments have led many to conclude that that the libel regime in the United Kingdom is in severe need of reform.[88] In March 2011, the UK Ministry of Justice published a "Draft Defamation Bill."[89] The consultation paper accompanying the bill noted concerns regarding "the detrimental effects the current libel regime has had on freedom of expression."[90] The bill also contained new procedures and provisions for reforming the law to strike the right balance between protection of freedom of speech and protection of reputation.[91]

In recent years, however, there has been a shift toward increased surveillance and police measures in the United Kingdom.[92] Interception and filtering measures have been

---

87. *See, e.g.*, Robinson, *supra* note 31, at 6 (describing the characteristics of a super-injunction); *see also, e.g.*, Somaiya, *supra* note 31, at A4 ("[T]he super-injunctions offer a way of stopping stories before they come out and are frequently served on multiple newspapers to pre-empt any possible publication . . . .").

88. *See* 27 Jan. 2010, PARL. DEB., (H.C.) (2010) 58 (U.K.), *available at* http://www.publications.parliament.uk/pa/cm200910/cmhansrd/cm100127/wmstext/100127m0001.htm (noting the establishment of a working group to address the government's "concerns about the possibility that [the United Kingdom's] libel laws are having a chilling effect on freedom of expression"). *See generally* MULLIS & SCOTT, *supra* note 83 (providing suggestions of ways to improve the libel regime in the United Kingdom).

89. JOINT COMMITTEE ON THE DRAFT DEFAMATION BILL, DRAFT DEFAMATION BILL, 2010–12, H.L. 203, H.C. 930–I (U.K.); *see* MINISTRY OF JUSTICE, DRAFT DEFAMATION BILL: CONSULTATION PAPER, 2011, Cm. 8020, at 3 (U.K.) (commenting on the proposal of the Draft Defamation Bill).

90. MINISTRY OF JUSTICE, *supra* note 89, at 5.

91. *Id.* at 5–7; *see* Press Release, Joint Select Comm., Parliament (U.K.), Joint Committee Publishes Report on Draft Defamation Bill (Oct. 19, 2011), *available at* http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-defamation-bill1/news/publication-report/ ("The unanimously-agreed report proposes many detailed amendments to the defenses available against libel claims, mainly designed to strike a fairer balance between the protection of reputation and freedom of speech.").

92. *See* Dominic Casciani, *Plan to Monitor All Internet Use*, BBC NEWS, Apr. 27, 2009, http://news.bbc.co.uk/2/hi/8020039.stm (describing a new initiative where communications firms would record all internet contacts between people as part of a modernization of UK police surveillance tactics); Ryan Gallagher & Rajeev Syal, *Met Police Using Surveillance System to Monitor Mobile Phones*, GUARDIAN (U.K), Oct. 30, 2011, at 8 (discussing covert surveillance technology that allows British police to shut off phones remotely, intercept communications, and gather data from users); Tom Kelly, *Revealed: Big Brother Britain Has More CCTV Cameras than China*, DAILY MAIL (U.K.),

implemented by state agencies as a means for a wide range of goals, including combating terrorism and preventing child abuse.[93] Critics have often referred to these types of regulations as "Big Brother plans" in a reference to George Orwell's novel *1984*.[94]

In 2000, Parliament passed the Regulation of Investigatory Powers Act ("RIPA"), which allowed public bodies to carry out surveillance and investigation.[95] RIPA can be invoked by government officials on the grounds of national security, and for purposes of detecting crime, preventing disorder, public safety, protecting public health, or in the interests of the economic well-being of the United Kingdom.[96] Many critics claim that RIPA was pushed through under the guise of fighting terrorism, internet crime, and pedophilia without being substantively debated in Parliament.[97] These critics say that the regulations are excessive and pose a threat to civil liberties.[98]

Aug. 11, 2009, http://www.dailymail.co.uk/news/article-1205607/Shock-figures-reveal-Britain-CCTV-camera-14-people—China.html (stating that Britain has 4.2 million closed circuit TV cameras, one per every fourteen people, that are used by the government).

93. *See IWF History*, INTERNET WATCH FOUND., http://www.iwf.org.uk/about-iwf/iwf-history (last visited May 25, 2012) (describing the purpose of internet surveillance); *see also* Casciani, *supra* note 92 ("Communications data is an essential tool for law enforcement agencies to track murderers, pedophiles, save lives and tackle crime." (quoting UK Home Secretary Jacqui Smith)); Gallagher & Syal, *supra* note 92, at 8 ("[The] products are designed to provide law enforcement, military, security agencies and special forces with the means to 'gather early intelligence in order to identify and anticipate threat and illegal activity before it can be deployed'.").

94. *See* Casciani, *supra* note 92 (expounding the dangers of "big brother databases" that store massive about of information about users); Kelly, *supra* note 92 ("Big Brother Britain has more CCTV cameras than China."). George Orwell's *1984* is a dystopian novel set in a world of pervasive government surveillance and public mind control. GEORGE ORWELL, 1984 (1950).

95. Regulation of Investigatory Powers Act, 2000, c. 23 (Eng.).

96. *Id.* § 5(3).

97. *See* Yaman Akdeniz et al., *Regulation of Investigatory Powers Act 2000(1): BigBrother.gov.uk: State Surveillance in the Age of Information and Rights*, 2001 CRIM. L. REV. 73, 77–80 (criticizing parts of the Regulation of Investigatory Powers Act ("RIPA")); *see also* Gordan Rayner & Richard Alleyne, *Council Spy Cases Hit 1,000 a Month*, TELEGRAPH (U.K.), Apr. 12, 2008, at 1 ("Councils and other public bodies are using legislation designed to combat terrorism in order to spy on people, obtain their telephone records and find out who they are emailing.").

98. *See* Casciani, *supra* note 92 (noting that the government has gone too far in building a culture of surveillance and calling for change); *see also* Akdeniz et al., *supra* note 97, at 79 (claiming that RIPA is overly broad in several respects); John Ozimek, *RIPA Ruling Closes Encryption Key Loophole*, REGISTER (U.K.), Oct. 14, 2008,

The United Kingdom has faced many of the same debates as those in the United States over the proper role of internet surveillance and regulation.[99] Because there is no written constitution in the United Kingdom, however, there is a lack of guidance in legal authority.[100] A House of Commons report acknowledged the limited body of case law on freedom of expression and privacy and recommended that, until major reforms are made, the common law should remain the basis upon which disputes are resolved.[101] This has resulted in a conflicting message and a haphazard approach to regulation by the government.[102]

---

http://www.theregister.co.uk/2008/10/14/ripa_self_incrimination_ruling/ ("Critics of RIPA continue to argue that the law is over-broad and capable of bringing about serious injustice.").

99. *See, e.g.*, Akdeniz et al., *supra* note 97, at 79 (arguing that legislation in the United Kingdom is overly broad); Gallagher & Syal, *supra* note 92, at 8 (discussing the debate over surveillance measures).

100. *See* Dan Sabbagh, *Tories Torn over Regulating Social Media*, GUARDIAN (U.K.), Aug. 24, 2011, at 16 (stating that British politicians have struggled to contend with Twitter, Facebook, and other social media in a time of crisis without a written constitution). *See generally* Simon Sellars, *Online Privacy: Do We Have It and Do We Want It? A Review of the Risks and UK Case Law*, 33 EUR. INTELL. PROP. REV. 9 (2011) (providing an overview of the issues that arise when attempting to regulate social media).

101. *See* COMMITTEE ON CULTURE, MEDIA, AND SPORT, COMMUNICATIONS REFORM: CONTEXT AND RATIONALE, 2001, H.C. 161-I, ¶ 16 (U.K.), *available at* http://www.publications.parliament.uk/pa/cm200001/cmselect/cmcumeds/161/16103.htm ("The White Paper does accept that the government must have a clear policy framework for 'this rapidly developing sector, which will be so central to our economy, democratic life, culture, entertainment and education,' but does not itself offer such a framework."); Sellars, *supra* note 100, at 9–10 ("The House of Commons Culture, Media and Sport Select Committee report . . . acknowledges the limited body of case law on freedom of expression and privacy, but declines to recommend legislative intervention. The Committee believes that the lack of unity on the part of the media industry and the 'infinitely different circumstances which can arise in different cases' mean that the flexibility of the common law should, for the time being, remain the basis upon which disputes are resolved.").

102. *See* MULLIS & SCOTT, *supra* note 83, at 2 (criticizing the haphazard approach to regulation of the libel regime in the United Kingdom); Sabbagh, *supra* note 100, at 16 (comparing the response to super-injunctions, where the government desired less regulation, with the News International tabloid phone-hacking crisis of 2011, where the government stated there should be more).

3. The Internet Phenomenon: Egypt

Eventually, the Internet's reach extended to less-technologically advanced countries such as Egypt.[103] The typical debates and issues took on new meaning in countries with drastically different understandings of accepted norms and standards of internet governance.[104] In 1971, the Arab Republic of Egypt adopted a democratic constitution.[105] Specifically, Article 47 stated: "Freedom of opinion is guaranteed. Every individual shall have the right to express his opinion and to disseminate it verbally, in writing, illustration or by other means within the limits of the law."[106] Articles 47 and 48 also provided for freedom of opinion and freedom of press.[107] In 1982, Egypt became a party to the International Covenant on Civil and Political Rights.[108] While these steps appear to establish Egypt as a democratic nation, many believe that they were merely "window-dressing" as the Egyptian government attempted to promote its legitimacy.[109]

---

103. *See* HUMAN RIGHTS WATCH, FALSE FREEDOM: ONLINE CENSORSHIP IN THE MIDDLE EAST AND NORTH AFRICA 17–26 (2005) (presenting an introduction to the Internet in Egypt).

104. *See, e.g.*, *id.* at 29–30 (citing examples of people who have been detained for things they wrote about on the Internet); OPENNET INITIATIVE, INTERNET FILTERING IN EGYPT 1, 4 (2009), *available at* http://opennet.net/sites/opennet.net/files/ONI_Egypt_2009.pdf (describing the problems the Egyptian government faced when regulating the Internet).

105. CONSTITUTION OF THE ARAB REPUBLIC OF EGYPT, 11 Sept. 1971, *as amended*, May 22, 1980, May 25, 2005, March 26, 2007.

106. *Id.* art. 47.

107. *Id.* arts. 47–48.

108. *International Covenant on Civil and Political Rights–Signatures, Accessions, Successions, Ratifications*, U.N. TREATY COLLECTION, http://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en (last visited May 25, 2012); *see* International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR]; *see also* HUMAN RIGHTS WATCH, *supra* note 103, at 37–38 (stating that Egypt is a party to the International Covenant on Human and Political Rights).

109. TAMIR MOUSTAFA, THE STRUGGLE FOR CONSTITUTIONAL POWER: LAW, POLITICS, AND ECONOMIC DEVELOPMENT IN EGYPT 7–8 (2007) (describing how the Egyptian government signed and ratified international conventions as "window-dressing" to attract economic development, with no expectation that they would someday be used to enforce rights); *see also* OPENNET INITIATIVE, *supra* note 104, at 4 ("Despite the government's initiatives to encourage internet use, the Egyptian authorities continue to place restrictions on how Egyptians use the Internet.").

The Internet became available to the Egyptian public in 1996.[110] The Egyptian government initially pursued an ambiguous policy in regards to the Internet, seeking to expand Egyptians' access to the Internet on the one hand while enforcing legislation criminalizing the freedom of expression on the other.[111] The imposition of emergency law gave the president broad powers on the grounds of protecting public safety and national security.[112] In addition, all ISPs passed through the state-run telecommunications company, Telecom Egypt, which facilitates government surveillance.[113] As a result, the Egyptian government found itself in the precarious position of attempting to respect democracy-minded internet principles and norms while still trying to control all aspects of society.[114]

The Ministry of Communications and Information Technology ("Ministry of Communications") was established in October 1999 with the intent to grow the country's technological infrastructure.[115] The Ministry of Communications launched several programs from 2002–2005, such as the Free Internet Program and the PC for Every Home program, seeking

---

110. *See* HUMAN RIGHTS WATCH, *supra* note 103, at 17–21 (describing the introduction of the Internet to Egypt); *see also* Amir Hatem Ali, *The Power of Social Media in Developing Nations: New Tools for Closing the Global Digital Divide and Beyond*, 24 HARV. HUM. RTS. J. 185, 208 (2011) ("The Internet was introduced in Egypt in 1993 and was commercialized in 1996, after which the Internet in Egypt underwent a period of substantial growth.").

111. *See* HUMAN RIGHTS WATCH, *supra* note 103, at 17–18 (describing the initial approach that the Egyptian government took in regulating the Internet); *see also* Ali, *supra* note 110, at 208–09 (tracing the changing response of the Egyptian government).

112. *See* HUMAN RIGHTS WATCH, *supra* note 103, at 41 (explicating the president's powers under emergency law); *see also* Daniel Williams, *Egypt Extends 25-Year-Old Emergency Law. Mubarak Had Vowed to Replace Far-Reaching Measure; U.S. Push for Reform Seen Easing*, WASH. POST, May 1, 2006, at A13 (describing Egypt's emergency law and its unpopularity with the public).

113. *See* HUMAN RIGHTS WATCH, *supra* note 103, at 24 ("Ignoring the fact that Egypt has no law that specifically prohibits visiting such sites, Issmat said that surveillance was easy because all internet service providers ("ISPs") passed through the state-run Egypt Telecom."); *see also* OPENNET INITIATIVE, *supra* note 104, at 2 (discussing the role of Telecom Egypt).

114. *See* HUMAN RIGHTS WATCH, *supra* note 103, at 17–18 (noting the competing interests of the Egyptian government); Ali, *supra* note 110, at 208–09 (tracing the changing response of the Egyptian government).

115. *See* HUMAN RIGHTS WATCH, *supra* note 103, at 19 (tracing the ways the Egyptian government initially sought to spread technology); *see also* OPENNET INITIATIVE, *supra* note 104, at 2 (describing the Egyptian government's internet initiative).

to make the Internet more affordable and more widely available.[116] Critics, however, argued that the Ministry was simply the propaganda arm of President Hosni Mubarak's regime.[117]

In September 2002, Egypt's Interior Ministry formed the General Administration for Information and Documentation ("GAID") to police the Internet.[118] In March 2004, the Department for Confronting Computer and Internet Crime was formed.[119] In 2008, rumors persisted of a special division called the State Security Investigation Police for Facebook.[120] Early on, these units worked to censor internet pornography.[121] The units

116. *See* HUMAN RIGHTS WATCH, *supra* note 103, at 19 (discussing the establishment of several programs as a means of spreading technology); *see also* Press Release, ITIDA, Dr. Kamel Witnesses Agreement Signing to Spread PC for Every Home Initiative Nationwide (Aug. 25, 2008), *available at* http://www.docstoc.com/docs/74366977/Kamel-Witnesses-Agreement-Signing-to-Spread-PC—Internet-Service- (describing the "PC For Every Home" initiative, whereby families will be able to pay for computers on credit via a monthly surcharge on their telephone bills).

117. *See Military Rulers Ignore Plural Voices*, IFEX (July 27, 2011), http://www.ifex.org/egypt/2011/07/27/military_ignore_plural_voices/ ("Long seen by journalists as the propaganda arm of Mubarak's regime, scrapping [the Ministry of Communications and Technology] was a key demand of members of the 18-day revolution . . . ."); *see also* FREEDOM HOUSE, FREEDOM ON THE NET 2011: EGYPT 5–8 (2011), *available at* http://www.freedomhouse.org/sites/default/files/inline_images/Egypt_FOTN2011.pdf (discussing the ways that the Ministry of Communications and Technology has responded to the spread of social media sites).

118. *See* HUMAN RIGHTS WATCH, *supra* note 103, at 24 (discussing how the department monitored the Internet in real time, seeking out and arresting those who went to pornographic sites, despite the fact that Egypt had no law prohibiting it); LEILA HASSANIN, GLOBAL INFO. SOC'Y WATCH, EGYPT, 122 n.16 (2009), *available at* http://www.giswatch.org/sites/default/files/Egypt.pdf ("[The General Administration for Information and Documentation] was formed in 2002 by the Egyptian Ministry of Interior and has been policing the internet ever since.").

119. *See* HUMAN RIGHTS WATCH, *supra* note 103, at 24 ("In March 2004, the government-owned daily *al-Ahram* first reported the existence of another specialized unit within the Interior Ministry, the Department for Confronting Computer and Internet Crime."); *see also* GAMAL EID, THE INTERNET IN THE ARAB WORLD: A NEW SPACE OF REPRESSION? (2004), *available at* http://www.anhri.net/en/reports/net2004/index.shtml (discussing the establishment of the Department for Confronting Computer and Internet Crime).

120. *See Rumors of a Facebook Block Persist in Egypt*, *supra* note 1 (noting the rumors of a special Facebook division of the police force); *see also* OPENNET INITIATIVE, *supra* note 104, at 4 ("Some also believe there is a special division called the State Security Police for Facebook.").

121. *See* HASSANIN, *supra* note 118, at 122 n.16 (introducing the General Administration for Information and Documentation, an organization formed by the Egyptian Ministry of Interior that was charged with policing the Internet against pornography); *see also* OPENNET INITIATIVE, *supra* note 104, at 5 (discussing the ways the nation filters pornography).

also have detained bloggers and political activists for a variety of reasons, sometimes without charging them with a crime.[122] Relying on emergency law, the authorities have applied broad power in detaining people they suspected of criminal activity.[123] Governments in Egypt and other developing nations continue to struggle with the growth of the Internet and the growing expectations that established norms will be respected.[124]

B. *The Emergence of Internet Norms and Standards*

Norms and standards developed simultaneously with the growth of the Internet and provided the foundation for modern conceptions of internet governance.[125] The Working Group on Internet Governance ("WGIG"), a group established by the United Nations to make proposals for action on the governance of the Internet, defines internet governance as the "development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."[126] As technology improves, the exigencies of internet

---

122. *See* OPENNET INITIATIVE, *supra* note 104, at 3–4 (giving examples of activist bloggers held by the authorities); *see also* HUMAN RIGHTS WATCH, *supra* note 103, at 29–30 (providing the example of Ashraf Ibrahim, who was held for nearly four months before being charged with "harming Egypt's reputation by spreading abroad false information regarding the internal affairs of the country to foreign bodies—human rights organizations—which includes, contrary to the truth, violations of human rights within the country").

123. *See* HUMAN RIGHTS WATCH, *supra* note 103, at 24–25 (discussing the detention of individuals under the emergency law); OPENNET INITIATIVE, *supra* note 104, at 3–4 (giving examples of activist bloggers held by the authorities); *see also infra* Part II.C (discussing abuses by the Egyptian government).

124. *See* Ali, *supra* note 110, at 185–86 (discussing the problems that the Egyptian government has faced as internet use has become more pervasive); HUMAN RIGHTS WATCH, *supra* note 103, at 24–25 (presenting examples of incidents involving internet bloggers); OPENNET INITIATIVE, *supra* note 104, at 3–4 (describing steps taken by the Egyptian government to control the Internet).

125. *See* Wu, *supra* note 10, at 663 ("[I]t is useful to think of the Internet less as a place and more as a regime of transnational norms and rules (a logical counterpart to transnational law) that regulates international interactions between individuals."); *see also* Lemley, *supra* note 10, at 1260 (discussing the existence of norms and standards that might be thought of as true private ordering: the social relationships that individuals and groups form that operate outside of the law).

126. World Summit on the Information Society, *supra* note 33, ¶ 10 (defining internet governance); *see* Press Release, United Nations, United Nations Established

governance change.[127] Yet, while internet standards continue to evolve, their underlying values of transparency, freedom of expression, and privacy persist.[128]

As a result of its development in the United States, the US government unilaterally controlled the Internet's initial architecture and infrastructure.[129] This also means that the norms and standards that developed reflected those found in the United States.[130] Freedom of expression and privacy are rooted in the US Constitution.[131] American jurisprudence and policy have further ingrained these tenets.[132] Private groups,

---

Working Group On Internet Governance, PI/1620 (Nov. 11, 2004) (announcing the creation of the group).

127. *See* World Summit on the Information Society, *supra* note 33, ¶ 8 ("During the 10 years in which the Internet evolved from a research and academic facility into 'a global facility available to the public', very different points of view emerged about the scope and mechanisms of Internet governance."). *Compare* Wu, *supra* note 10, at 649–50 (discussing Internet governance in light of the existing technology in 1997), *with* Sylvain, *supra* note 38, at 208–09 (describing policymaking in terms of broadband technology).

128. *See* World Summit on the Information Society, *supra* note 33, ¶¶ 13–28 (identifying the issues that continue to be relevant to internet governance); Sylvain, *supra* note 38, at 212–15 (describing the standards used by early internet engineers and discussing how agencies like the Federal Communications Commission continue to use the standards when regulating the Internet).

129. *See* World Summit on the Information Society, *supra* note 33, ¶ 15 (stating that the United States was initially responsible for the growth and development of the Internet); *see also* George Sadowsky, *The Internet Society and Developing Countries*, E-OTI: ONTHEINTERNET, Nov./Dec. 1996, http://www.isoc.org/oti/articles/1196/sadowsky.html ("It is true that the roots of the Internet in North America, coupled with the initial explosion of content in the same general region, currently make the Internet, and especially the World Wide Web, primarily a medium of expression in English.").

130. *See, e.g.*, OECD, *supra* note 32, ¶ 25 (citing the protection of privacy and individual liberties and the advancement of free flows of personal data as two essential basic values); Sadowsky, *supra* note 130 ("The culture of the Internet reflects its roots in the North American research community. . . . Important elements of that culture include broad freedom of expression and sharing of information.").

131. *See, e.g.*, U.S. CONST. amends. I, XIV; *see supra* Part I.A.1 (tracing the developments in internet law).

132. *See, e.g.*, Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552(a) (2006)) (governing the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies); Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (holding that the government cannot punish inflammatory speech unless it is intended to incite imminent lawless action); Griswold v. Connecticut, 381 U.S. 479, 484–85 (1965) (finding that a right to privacy could be found in the "penumbras" and "emanations" of other constitutional protections).

international organizations, and governmental agencies have applied these principles in establishing some semblance of internet governance.[133]

1. Establishing Norms: Technological and Engineering Groups

In the early days of the Internet, technological and engineering organizations were given almost exclusive responsibility over the direction of internet development.[134] These groups were responsible for determining the initial principles and standards that would guide the Internet's growth. [135] Each group has stressed the importance of transparency and openness when developing the Internet.[136] As a result, users now expect both freedom of expression and privacy when partaking in social media.[137]

The Internet Engineering Task Force's ("IETF") is a group of network designers, operators, vendors, and researchers.[138] Its

---

133. *See infra* Part II (setting forth the ways different groups have established internet norms and standards).

134. *See* KAHN & CERF, *supra* note 34, at 28–34 (outlining the responsibilities of different organizations); Sylvain, *supra* note 38, at 212 ("The network-design features that have made the Internet an especially transformative medium are captured in three principles championed by the IETF, the preeminent technical standard-setting organization for the industry . . . .").

135. *See The Tao of the IETF: A Novice's Guide to the Internet Engineering Task Force*, INTERNET ENGINEERING TASK FORCE, http://www.ietf.org/tao.html#anchor5 (last visited May 25, 2012) (stating that "[t]he goal of the IETF is to have its standards widely used and validated in the marketplace"); *see also* KAHN & CERF, *supra* note 34, at 30–31 (outlining the responsibilities of different organizations).

136. *See, e.g.*, *ICANN Accountability & Transparency*, INTERNET CORP. ASSIGNED NAMES & NUMBERS, http://www.icann.org/en/news/in-focus/accountability (last visited May 25, 2012) (presenting the goals of the organization); *The IETF Standards Process*, INTERNET ENGINEERING TASK FORCE, http://www.ietf.org/about/standards-process.html (last visited May 25, 2012) (listing openness and fairness as goals of the IETF Standards Process).

137. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESS AND POLICYMAKERS; PRELIMINARY FTC STAFF REPORT 53 (2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (recognizing users' expectations when proposing a new framework for regulations); Letter from Michael Richter, Chief Privacy Counsel, Facebook, to the Fed. Trade Comm'n (Feb. 18, 2011), *available at* http://www.ftc.gov/os/comments/privacyreportframework/00413-58069.pdf [hereinafter Letter from Facebook to the FTC] (stressing the importance of the FTC respecting users' expectations when crafting policy).

138. *See About the IETF*, INTERNET ENGINEERING TASK FORCE, http://www.ietf.org/about/ (last visited May 25, 2012) (describing the IETF); *see also* Sylvain, *supra* note 38,

mission is to make the Internet work better by producing technical documents that influence the way people design, use, and manage the Internet.[139] The group is organized into thousands of working groups that deal with specific topics.[140] Throughout its existence, the IETF has followed the same guiding principles: openness and fairness.[141] The goal for these original architects of the Internet was to avoid centralized governmental control.[142] According to the IETF, government's only obligation is "to stay out of the way and eschew censorship."[143]

Another group that works to preserve the openness, transparency, and stability of the Internet is the Internet Corporation for Assigned Names and Numbers ("ICANN").[144]

---

at 206 (defining the IETF as a private self-regulatory organization comprised of geographically dispersed engineers and application designers).

139. *Mission Statement*, INTERNET ENGINEERING TASK FORCE, http://www.ietf.org/about/mission.html (last visited May 25, 2012); *see also* Sylvain, *supra* note 38, at 206 (describing the IETF as a "private self-regulatory organization[] for which decentralization, user empowerment, and interoperability [is] a priority").

140. *See About the IETF*, *supra* note 138 ("The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet."); *see also* Sylvain, *supra* note 38, at 206 (defining the IETF as a private self-regulatory organization comprised of geographically dispersed engineers and application designers).

141. *See The IETF Standards Process*, *supra* note 136 (mentioning openness and fairness as major guiding principles of the IETF Standards Process); *see also* Sylvain, *supra* note 38, at 217 ("These authorities [referring to the IETF], the FCC explained, show that, first, the Internet is meant to afford users access to the content and applications of their choice, and, second, its original engineers and programmers wanted disparately located users to be able to collaborate and comment on a common project.").

142. *See* A. Michael Froomkin, *Habermas@Discourse.net: Toward a Critical Theory of Cyberspace*, 116 HARV. L. REV. 749, 811 (2003) ("[The] Internet is for everyone—but it won't be if Governments restrict access to it, so we must dedicate ourselves to keeping the network unrestricted, unfettered and unregulated."); *see also* Sylvain, *supra* note 38, at 212 (presenting interoperability as a principle championed by the IETF and defining it as "the principle that independent computer networks are not barred from freely exchanging information with others").

143. Froomkin, *supra* note 142, at 811; *see* Sylvain, *supra* note 38, at 212 (referring to user empowerment as the "notion that nothing in the maintenance of the physical network may interfere with any user's access to all of the services, applications, and other users of her choice").

144. *See Welcome to ICANN*, INTERNET CORP. ASSIGNED NAMES & NUMBERS, http://www.icann.org/en/about/welcome (last visited May 25, 2012) (introducing the Internet Corporation for Assigned Names and Numbers ("ICANN")); *see also* KAHN & CERF, *supra* note 34, at 33 (providing a background to ICANN).

Formed in 1998, ICANN is a nonprofit corporation that oversees a number of Internet-related tasks including the use of internet names and numbers.[145] ICANN's goals include helping to preserve the operational stability of the Internet, to promote competition, and to achieve broad representation of the global internet community.[146]

These groups and others like them allow the Internet to function and have been vital to its growth.[147] From their initial guidance, international organizations began to develop new ideas concerning internet governance, building on the foundation laid by engineering groups like the IETF and ICANN.[148]

2. Adopting Norms: International Organizations

As the Internet's reach expanded, international organizations also have tried to establish some form of universal internet governance.[149] Numerous international agreements protect both freedom of expression and privacy.[150] Specifically, Article 19 of the International Covenant on Civil and Political Rights guarantees the right to freedom of expression, including the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in

---

145. *See Welcome to ICANN*, *supra* note 144 (presenting background on ICANN); *see also* KAHN & CERF, *supra* note 34, at 33 (providing a background to ICANN).

146. *See What Does ICANN Do?*, INTERNET CORP. ASSIGNED NAMES & NUMBERS, http://www.icann.org/en/about/participate/what (last visited May 25, 2012) (listing the goals of ICANN); *see also* KAHN & CERF, *supra* note 34, at 33 (providing a background to ICANN).

147. *See* KAHN & CERF, *supra* note 34, at 28–34 (describing the functions of different internet groups); Sylvain, *supra* note 38, at 206 (expressing the importance of technological organizations in developing the rules for network regulation).

148. *See infra* Part I.B.2 (explaining how international organizations helped to spread internet norms and standards).

149. *See generally, e.g.*, World Summit on the Information Society, *supra* note 33 (reporting on the state of internet governance on behalf of the United Nations ("UN")); World Summit on the Information Society, Geneva 2003–Tunis 2005, *Declaration of Principles: Building the Information Society; A Global Challenge in the New Millennium*, WSIS-03/Geneva/Doc/4-E (Dec. 12, 2003), *available at* http://www.itu.int/wsis/docs/geneva/official/dop.html [hereinafter WSIS Declaration of Principles] (presenting a set of Internet principles and standards).

150. *See, e.g.*, ECHR, *supra* note 80, arts. 8, 10, 213 U.N.T.S. at 230; ICCPR, *supra* note 108, arts. 17, 19, 999 U.N.T.S. at 177–78.

print, in the form of art, or through any other media."[151] Privacy is protected in Article 17, which states: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation." [152] Consequently, there is an understanding that it is equally important to protect both freedom of expression and privacy when dealing with internet governance internationally. [153] The United States, United Kingdom, and Egypt are all parties to the International Covenant on Civil and Political Rights.[154]

The United Nations has become one of the major actors working to institute a comprehensive understanding of internet governance. [155] It has established working groups and held conferences with the goal of establishing norms of internet governance to be used internationally.[156] For example, in 2000, the United Nations funded a workshop on the principles of freedom of expression.[157] During the workshop, the committee

---

151. ICCPR, *supra* note 108, art. 19, 999 U.N.T.S. at 178.

152. *Id.* art. 17, 999 U.N.T.S at 177.

153. *See* World Summit on the Information Society, *supra* note 33, ¶¶ 24–25 (listing freedom of expression and privacy rights as public policy issues that are relevant to Internet governance).

154. *See, e.g.*, *International Covenant on Civil and Political Rights–Signatures, Accessions, Successions, Ratifications*, *supra* note 108.

155. *See, e.g.*, World Summit on the Information Society, *supra* note 33, ¶¶ 1–6 (establishing a group to report on the state of Internet governance); ARTICLE 19, DEFINING DEFAMATION: PRINCIPLES OF FREEDOM OF EXPRESSION AND PROTECTION OF REPUTATION 2–3 (2000), *available at* http://www.article19.org/data/files/pdfs/standards/definingdefamation.pdf (prescribing principles of freedom of expression and protection of reputation following a workshop sponsored by the United Nations) [hereinafter DEFINING DEFAMATION].

156. *See, e.g.*, World Summit on the Information Society, *supra* note 33, ¶¶ 1–6 (establishing the Working Group while recognizing that the Internet is "a central element of the infrastructure of the emerging information society, while recognizing that there are differing views on the suitability of current institutions and mechanisms for managing processes and developing policies for the global Internet"); DEFINING DEFAMATION, *supra* note 155, at 2–3 (introducing freedom of expression and protection of reputation as important principles).

157. DEFINING DEFAMATION, *supra* note 155, at 1; *see* HOUSE OF COMMONS SELECT COMMITTEE ON CULTURE, MEDIA, AND SPORT, SUPPLEMENTARY WRITTEN EVIDENCE FROM ARTICLE 19 (2009) (U.K.), *available at* http://www.publications.parliament.uk/pa/cm200809/cmselect/cmcumeds/memo/press/ucm8902.htm (examining international standards relating to freedom of expression generally and then in the particular context of defamation laws, focusing mainly on the jurisprudence of the European Court of Human Rights).

reaffirmed the belief that "freedom of expression and the free flow of information . . . are of crucial importance in a democratic society, for the personal development, dignity and fulfillment of every individual, as well as for the progress and welfare of society, and the enjoyment of other human rights and fundamental freedoms."[158] In addition, the committee asserted that any restriction on freedom of expression must be subject to adequate safeguards against abuse as an aspect of the rule of law.[159]

In 2003 and 2005, the United Nations sponsored a two-part conference, called the World Summit on the Information Society ("WSIS").[160] Held in Geneva in 2003 and Tunis in 2005, the conference discussed issues relating to communication, information, and technology.[161] The WSIS Declaration of Principles was established, reaffirming the right to freedom of expression.[162] Relying on Article 19 of the Universal Declaration of Human Rights, the WSIS Declaration stated that the right includes "freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[163]

After the conference, several other groups emerged from the mandate of the WSIS.[164] The WGIG was formed in 2003 to

---

158. DEFINING DEFAMATION, *supra* note 155, at 2.

159. *Id.* at 3–4.

160. *See* G.A. Res. 56/183, pmbl., U.N. Doc. A/RES/56/183 (Jan. 31, 2002), *available at* http://www.itu.int/wsis/docs/background/resolutions/56_183_unga_2002.pdf (adopting a resolution calling for a world summit to "address the whole range of relevant issues related to the information society, through the development of a common vision and understanding of the information society and the adoption of a declaration and plan of action for implementation by governments, international institutions and all sectors of civil society"); WSIS Declaration of Principles, *supra* note 149 (discussing the role of the Working Group on Internet Governance ("WGIG") in determining an appropriate approach to internet governance).

161. *See generally* World Summit on the Information Society, *supra* note 33, ¶ 5 (mentioning the goals of the summit).

162. *See* WSIS Declaration of Principles, *supra* note 149, ¶ 4; *see also* World Summit on the Information Society, *supra* note 33, ¶¶ 13–36 (affirming the principles established at the summit).

163. WSIS Declaration of Principles, *supra* note 149, ¶ 4; *see also* World Summit on the Information Society, *supra* note 33, ¶¶ 13–36 (affirming the principles established at the summit).

164. *See* WSIS Declaration of Principles, *supra* note 149, ¶ 50 (mandating the creation of a working group on internet governance); World Summit on the

determine the public policy issues relevant to internet governance.[165] The group was asked to develop an understanding of the roles of governments, international organizations, the private sector, and civil society from developing and developed countries.[166] The United Nations also announced the establishment of the Internet Governance Forum in 2006, which brought together groups that represent governments, the private sector, and civil society to establish a policy dialogue on issues of internet governance.[167]

The Organisation for Economic Co-operation and Development ("OECD") is an example of an international economic organization that has played a role in shaping internet norms.[168] The OECD has formed a Group of Experts on Transborder Data Barriers and Privacy Protection that was instructed to develop guidelines on basic rules governing the protection of personal data and privacy across borders in order to enable coordination of national legislation.[169] The OECD

Information Society, *supra* note 33, ¶¶ 1–6 (providing an example of one of the groups that was formed after the summit).

165. *See* World Summit on the Information Society, *supra* note 33, ¶ 5 ("The WGIG has been asked, inter alia, to 'investigate and make proposals for action, as appropriate, on the governance of the Internet.'").

166. *See* World Summit on the Information Society, *supra* note 33, ¶ 4 (restating the mandate of the World Summit on the Information Society ("WSIS")); *see also* WSIS Declaration of Principles, *supra* note 149, ¶ 50 (mandating the creation of a working group on Internet governance).

167. *See About the Internet Governance Forum*, INTERNET GOVERNANCE F., http://www.intgovforum.org/cms/aboutigf (last updated May 24, 2012) (discussing the creation of the Internet Governance Forum); *see also Annan Announces UN Forum on Internet Governance*, GOV'T TECH., Mar. 3, 2006, http://www.govtech.com/e-government/Annan-Announces-UN-Forum-on-Internet.html ("Following up on an agreement reached on the contentious topic of Internet governance at the November World Summit on the Information Society (WSIS) in Tunis, United Nations Secretary-General Kofi Annan announced he would create a forum for 'a more inclusive dialog' on Internet policy.").

168. *See* Convention on the Organisation for Economic Co-Operation and Development, Dec. 14, 1960, 12 U.S.T. 1728, 888 U.N.T.S. 179 (creating the Organisation for Economic Co-operation and Development ("OECD")); *see also About the Organisation for Economic Co-operation and Development*, OECD, http://www.oecd.org/pages/0,3417,en_36734052_36734103_1_1_1_1_1,00.html (last visited May 25, 2012) (describing the OECD). The OECD was founded in the early 1960s to stimulate economic progress and world trade. *See About the Organisation for Economic Co-operation and Development*, *supra*.

169. *See* OECD, *supra* note 32, ¶¶ 25–26 (presenting the purposes of the principles); *see also* Soma et al., *supra* note 41, at 529 (mentioning the applications of the OECD Guidelines).

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the Communiqué on Principles for Internet Policy-Making contain guidelines and principles that stress privacy and freedom of expression as important norms that should be preserved.[170] The OECD focuses on eight privacy principles: (1) Collection Limitation, (2) Data Quality, (3) Purpose Specification, (4) Use Limitation, (5) Security Safeguards, (6) Openness, (7) Individual Participation, and (8) Accountability.[171] The guidelines eventually led to the European Union Data Protection Directive ("EU Directive"), which stated as a basic proposition that the joint goals of protecting personal privacy and avoiding restrictions on the free flow of personal data based on privacy concerns among member countries are essential to the evolution of the integrated market in Europe.[172]

These groups recognize the significance of countries committing to a set of core principles.[173] By taking norms and standards used by technological and engineering groups and applying them to questions of internet governance, they have provided for their widespread dissemination and adoption.[174] In

---

170. *See* OECD, *supra* note 32, ¶¶ 7–22 (listing the guidelines); *see also* OECD, COMMUNIQUÉ ON PRINCIPLES FOR INTERNET POLICY-MAKING (2011), *available at* http://www.oecd.org/dataoecd/40/21/48289796.pdf [hereinafter OECD COMMUNIQUÉ] (presenting principles on Internet policymaking).

171. *See* OECD COMMUNIQUÉ, *supra* note 170 (presenting principles on internet policymaking); Soma et al., *supra* note 41, at 529 (listing the eight privacy principles established by the OECD).

172. Council Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. L 281; *see* Raymond T. Nimmer, *European Data Protection*, 1 INFO. L., Nov. 2011, § 8:82 (explaining the basic proposition of the European Union Data Protection Directive ("EU Directive")).

173. *See* OECD COMMUNIQUÉ, *supra* note 170 (adopting a set of principles); *see also* World Summit on the Information Society, *supra* note 33, ¶¶ 13–36 (presenting principles that should be adopted in developing a system of internet governance); *About the Internet Governance Forum*, *supra* note 167 (citing critical internet norms and standards that should be followed). In 2012, the European Commission proposed a major reform of the EU legal framework of the protection of personal data to strengthen online privacy rights. *See Protection of Personal Data*, EUR. COMMISSION, http://ec.europa.eu/justice/data-protection/index_en.htm (last updated Apr. 4, 2012).

174. *See* OECD COMMUNIQUÉ, *supra* note 170 (adopting a set of principles); *see also* World Summit on the Information Society, *supra* note 33, ¶¶ 13–36 (outlining principles for adoption in developing a system of internet governance); *About the Internet Governance Forum*, *supra* note 167 (citing critical Internet norms and standards that should be followed).

turn, the principles of openness, freedom of expression, transparency, and privacy became ubiquitous on the Internet.[175]

3. Applying Norms to Policy: Governmental Agencies

In the United States, governmental agencies such as the FCC and the FTC have adopted policies that reflect the norms to which groups such as the Internet Engineering Task Force ("IETF") were committed.[176] In 1998, the FTC introduced five core principles of privacy protection: (1) Notice/awareness, (2) Choice/consent, (3) Access/participation, (4)Integrity/security, and (5) Enforcement/redress.[177] The principles were the result of a series of reports, guidelines, and model codes that represent widely accepted norms concerning fair information practices.[178] As the Internet Society has stated, "users expect internet traffic to be conveyed in a manner that is independent of its source, content, or destination, and in a manner that respects their privacy."[179] Likewise, governmental agencies have accepted these principles and crafted their policies in a way that respects them.[180]

---

175. *See, e.g.*, World Summit on the Information Society, *supra* note 33, ¶¶ 13–36 (accepting the norms of openness, freedom of expression, transparency, and privacy as established principles and applying them to a broad concept of internet governance); *see also* Letter from Facebook to the FTC, *supra* note 137 (asserting that these principles must be respected and followed).

176. *See* Sylvain, *supra* note 38, at 216 ("The law governing the provision of wireline broadband service . . . amounts to little more than a policy of liberal deference to Internet engineers, programmers, and entrepreneurs."); *see also* Saul Hansell, *F.C.C. Vote Sets Precedent on Unfettered Web Usage*, N.Y. TIMES, Aug. 2, 2008, at C1 (discussing how the FCC sought to make ensure that Comcast was following industry practices).

177. *See* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7–11 (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf (listing the FTC's privacy principles); *see also* Soma et al., *supra* note 41, at 530 (presenting the five core principles of privacy protection).

178. *See* FED. TRADE COMM'N, *supra* note 177, at ii ("In this report, the Commission summarizes widely-accepted principles regarding information collection, use, and dissemination."); W. Scott Blackmer et al., *Online Consumer Data Privacy Regulation in the U.S.*, 3 ELECTRONIC BANKING L. & COM. REP. 1, 1–3 (1999) (describing the background behind the FTC privacy principles).

179. INTERNET SOC'Y, *supra* note 32, at 4; *see* Citron, *supra* note 70, at 834–37 (discussing individuals' privacy expectations for the government).

180. *See, e.g.*, FED. TRADE COMM'N, *supra* note 137, at 3 (using accepted Internet norms in proposing a framework for protecting privacy on the Internet); FED. TRADE COMM'N, *supra* note 177, at 7 (presenting privacy principles based on accepted Internet norms).

In 2010, the FTC released a proposed privacy framework.[181] The proposal was intended to inform policymakers, including Congress, as they develop policies and potential legislation regarding privacy, and also to guide industry as it develops more effective self-regulatory guidelines and practices.[182] The proposal also documented the FTC's longstanding efforts to protect privacy and called for the systemic implementation of procedural safeguards.[183] The FTC received over 400 comments on the proposal from individuals, organizations, and corporations including Facebook, Google, IBM, and Microsoft.[184] The majority of these responses applauded the FTC's efforts to reexamine the balance between the public's interest in sharing information against their interest in maintaining control over that information.[185]

Some government authorities rationalize that security also is an established internet norm that they are seeking to preserve when contemplating internet regulations.[186] In almost all of these cases, however, "security" refers to *network* security rather than physical security.[187] For example, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data mention that having security safeguards is an important

---

181. *See* FED. TRADE COMM'N, *supra* note 137, at 39; *see also* Richard L. Santalesa, *What's Next for the FTC's Proposed Privacy Framework?*, INFO. L. GRP. (Mar. 23, 2011), http://www.infolawgroup.com/2011/03/articles/data-privacy-law-or-regulation/whats-next-for-the-ftcs-proposed-privacy-framework/ (discussing the proposed privacy framework).

182. *See* FED. TRADE COMM'N, *supra* note 137, at i.

183. *See id.* at v, 3–19 (explaining the efforts of the FTC to protect privacy, and stating that: "Companies also should implement and enforce procedurally sound privacy practices throughout their organizations . . . the time has come for industry to implement them systematically.").

184. *See* Santalesa, *supra* note 181 (describing the groups that responded to the FTC's Proposed Privacy Framework); *see also* Letter from Facebook to the FTC, *supra* note 137 (providing an example of the types of responses).

185. *See* Santalesa, *supra* note 181 (examining the responses of organizations such as Google, IBM, and Facebook, and finding that while there were some criticisms, generally, these companies agreed that the FTC was on the right track); *see also* Letter from Facebook to the FTC, *supra* note 137 (agreeing that the groups must reexamine the balance between freedom of expression and privacy).

186. *See infra* Part II (examining specific events in Egypt, the United Kingdom, and the United States).

187. *See* OECD, *supra* note 32, ¶ 11 (referring to the security of personal data); World Summit on the Information Society, *supra* note 33, ¶ 79 (asserting that security measures should protect privacy and personal data).

principle.[188] The guidelines deal with the protection of personal data by reasonable security safeguards, however, and therefore support a privacy norm rather than a security norm.[189]

Additionally, the WGIG refers to the stable and secure functioning of the Internet when discussing security. [190] According to the group, security is the protection of privacy and other human rights.[191] The WGIG goes further to warn that measures taken by governments on grounds of security can lead to violations of the provisions for freedom of expression as contained in the Universal Declaration of Human Rights and in the WSIS Declaration of Principles.[192]

The FTC also refers to safety in its discussion on internet principles.[193] According to the FTC, the greatest safety risk is presented by the posting of personal identifying information by and about children.[194] Additionally, the FTC mentions security as a norm in the banking and financial industries, and limits the use of the principle to protecting these industries' sensitive information. [195] Notwithstanding these discrepancies, some

---

188. *See* OECD, *supra* note 32, ¶ 11 ("Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.").

189. *See* OECD, *supra* note 32, ¶ 56 (discussing security in terms of protecting privacy).

190. *See* World Summit on the Information Society, *supra* note 33, ¶ 6 ("In particular, the WSIS principle relating to the stable and secure functioning of the Internet was judged to be of paramount importance.").

191. *See* Universal Declaration of Human Rights, pmbl., G.A. Res. 217 (III) A, U.N. Doc. A/Res/217(III) (Dec. 10, 1948) (recognizing freedom of speech as a fundamental human right); *see also* World Summit on the Information Society, *supra* note 33, ¶ 79 (asserting that security measures should provide for the "appropriate protection of privacy, personal data and other human rights"); WSIS Declaration of Principles, *supra* note 149, ¶ 55 (reaffirming the WSIS's commitment to the principles of freedom of the press and freedom of information).

192. *See* World Summit on the Information Society, *supra* note 33, ¶ 24 (warning that any action taken by governments on the ground of security may violate international treaties).

193. *See* FED. TRADE COMM'N, *supra* note 177, at ii ("These core principles require that . . . the data collector take appropriate steps to ensure the *security* and integrity of any information collected.").

194. *See id.* at 5 (stating that sites should assure that children's data is secure from unauthorized uses or disclosures).

195. *See id.* at 16 ("Only the banking and financial industry association guidelines, and the individual reference services guidelines, make any reference to security issues. These guidelines call generally for appropriate security procedures, including the limitation of employee access to data.").

government groups continue to maintain that security is an established internet standard that should be respected.

II. *CURRENT EVENTS AND GOVERNMENTAL POLICIES: EGYPT, THE UNITED KINGDOM, AND THE UNITED STATES*

As internet use has become more prevalent, governments have begun to formulate procedures regarding internet interference. Part II describes the current governmental policies in Egypt, the United Kingdom, and the United States regarding internet and, specifically, social media regulation. Part A discusses attempts made by the Egyptian government to control the Internet by examining the events of the summer of 2011. Part B examines issues the UK government faced when regulating social media sites both before and after the riots of the summer of 2011. Part C analyzes problems that have arisen in the United States as the government tries to determine its role in regulating social media.

A. *Egypt: The Revolution of 2011 and Its Aftermath*

> "*Freedom of expression means you can speak up, criticize, and write what you want, as long as it is not against the law.*"
>
> *–Hosni Mubarak, former President of Egypt*[196]

Although the provisions of the Constitution of Egypt and the International Covenant on Civil and Political Rights seemingly provided for the freedom of expression and privacy, the imposition of emergency law in Egypt severely limited their reach.[197] Emergency law was imposed in Egypt in 1967, allowing

---

196. MOUSTAFA, *supra* note 109, at 118 (quoting an interview with former Egyptian President Hosni Mubarak).

197. CONSTITUTION OF THE ARAB REPUBLIC OF EGYPT, 11 Sept. 1971, *as amended,* May 22, 1980, May 25, 2005, March 26, 2007, arts. 47–49; ICCPR, *supra* note 108, arts. 17, 19, 999 U.N.T.S. at 177–78; *see* NATHAN J. BROWN, THE RULE OF LAW IN THE ARAB WORLD: COURTS IN EGYPT AND THE GULF 122–25 (1997) (discussing emergency law in Egypt); *see also* Sarah Carr, *Journalists Challenge Egypt's Exceptional Laws at Seminar*, DAILY STAR (Egypt) (Aug. 1, 2008, 2:00 AM), http://www.dailystaregypt.com/article.aspx?ArticleID=15464 (last visited May 25, 2012) ("These laws have gradually been added to over the years so that now you have layers and layers of oppressive legislation.").

the government to rule under a state of emergency.[198] In May 1980, the state of emergency was lifted, but following the assassination of President Anwar Al-Sadat, it was reimposed on October 6, 1981, and has been regularly renewed since then.[199] Many constitutional rights were suspended, police powers were extended, and the government was given the power of censorship.[200] While the declared objective of the legislation was to better enable the government and security forces to uncover militant Islamists, the laws effectively allowed the government to maintain their power.[201]

The growth of the Internet in Egypt reflected the young population's "thirst for new technology."[202] Social networking provided many Egyptians with a venue to express themselves, organize around political and social causes, and circulate

198. *See* HUMAN RIGHTS WATCH, *supra* note 103, at 39 ("Egypt's Emergency Law (Law No. 162 of 1958 as amended), in effect almost continuously since 1967, gives the president broad powers . . . ."); *see also* Submission from the Int'l Comm'n of Jurists (ICJ) to the Universal Periodic Review of Egypt, 7th Sess. of the Working Grp. on the Universal Periodic Review (Feb. 8–19, 2010), U.N. Human Rights Council 1 (Aug. 2009), *available at* http://www.icj.org/IMG/UPRSubmission-Egypt.pdf [hereinafter ICJ Submission] (providing an introduction to the emergency law in Egypt).

199. *See* ICJ Submission, *supra* note 198, at 1 (tracing the use of the emergency law); *see also* HUMAN RIGHTS WATCH, *supra* note 103, at 39 n.152 ("The Emergency Law was imposed in 1967, in the wake of the Arab-Israeli war. It was lifted briefly in May 1980 after the implementation of the Camp David accords, then reinstated after President Anwar al-Sadat's assassination in October 1981.").

200. *See* Carr, *supra* note 197 ("The emergency law in force since the declaration of the state of emergency grants the administrative authority powers to search, arrest and detain individuals without the supervision of judicial bodies."); Williams, *supra* note 112, at A13 ("No potential reform measure had been more anticipated than cancellation of the emergency law, which permits indefinite detention without trial and hearings of civilians by military courts, prohibits gatherings of more than five people, and limits speech and association."); *see also* ICJ Submission, *supra* note 198, at 2–4 (detailing the abuses of power that have occurred under emergency law).

201. *See* MOUSTAFA, *supra* note 109, at 137 (criticizing the emergency laws); *see also* HUMAN RIGHTS WATCH, *supra* note 103, at 39 ("Law 97/1992, known as the Law to Combat Terrorism, gives the government broader powers to combat political violence, and criminalizes forms of non-violent opposition.").

202. *See* Noam Cohen, *In Egypt, a Thirst for Technology and Progress*, N.Y. TIMES, July 21, 2008, at C3 ("In Egypt, where half the population is under 25, there is a thirst for new technology and a chance to escape the backward conditions its young people have been born into."); *see also Rumors of a Facebook Block Persist in Egypt*, *supra* note 1 ("The social networking powerhouse has become a venue for bloggers to express themselves, organize around political and social causes, and circulate information that would be considered taboo in other media.").

information.[203] For example, in April of 2008, activists in Egypt used Facebook to organize strikes and protests days before municipal elections.[204] Facebook groups played a significant role in recruiting supporters and increasing turnout for the demonstrations.[205]

After the strike, the Egyptian government asked mobile phone companies to block service to certain subscribers under the pretext of security.[206] Egyptian authorities also threatened to block access to the Facebook site within the country.[207] In February 2009, the telecommunications company Vodafone revealed that it had handed over communications data to the Egyptian authorities in response to government demands.[208] The

---

203. *See Rumors of a Facebook Block Persist in Egypt*, *supra* note 1 ("The social networking powerhouse has become a venue for bloggers to express themselves, organize around political and social causes, and circulate information that would be considered taboo in other media."); *see also* Mariam Fam, *Egyptian Political Dissent Unites Through Facebook*, WALL ST. J., May 5, 2008, at A9 ("Facebook [in Egypt] has evolved into more than just a social networking Web site: it is one of the latest tools for political dissent in Egypt.").

204. *See Rumors of a Facebook Block Persist in Egypt*, *supra* note 1 ("The general strike that unfolded in Egypt on April 6 was advertised on a Facebook group [called the April 6 Youth Movement], which attracted more than 70,000 members and played a significant role in recruiting supporters and increasing turnout for the demonstrations."); *see also* Fam, *supra* note 203, at A9 (discussing the popularity of the April 6 Youth Movement group).

205. *See Rumors of a Facebook Block Persist in Egypt*, *supra* note 1 (describing a popular Facebook group that played a large role in recruiting supporters and increasing turnout for the demonstrations); *see also* Fam, *supra* note 203, at A9 (discussing the role that Facebook played in organizing for the strike).

206. *See* Cynthia Johnston, *Egypt Asks Mobile Firms to Bar Anonymous Users*, REUTERS, May 5, 2008, http://ca.reuters.com/article/technologyNews/idCAL056268520080505 (reporting on Egypt's request to mobile phone companies to block service to anonymous subscribers as a public security measure); *see also* OPENNET INITIATIVE, *supra* note 104, at 4 ("Vodafone revealed in February 2009 that it handed over communications data to the Egyptian authorities that may have been used to help identify rioters who were protesting during the April 2008 bread crisis.").

207. *See Rumors of a Facebook Block Persist in Egypt*, *supra* note 1 ("Egyptian authorities are threatening to block access to Facebook within the country . . . the rumors continue to circulate and the potential to make Facebook disappear from computer monitors across Egypt is real."); *see also* OPENNET INITIATIVE, *supra* note 104, at 4 (stating that the Egyptian government considered blocking Facebook after the April 6 strike).

208. *See* Helmi Noman, *Can They Hear Me Now? (On ICT Regulations, Governments, and Transparency)*, OPENNET INITIATIVE (Feb. 24, 2009), http://opennet.net/blog/2009/02/can-they-hear-me-now-on-ict-regulations-governments-and-transparency ("On February 11, Vodafone's global head of content standards . . . revealed that Vodafone handed over communications data to the Egyptian authorities in response to

data may have been used to help identify people involved in the 2008 riots.[209] In January 2011, people began using Facebook and social media to organize protests around Egypt.[210] On January 25, 2011, tens of thousands of protesters gathered in and around Tahrir Square in Cairo, demanding an end to the rule of President Hosni Mubarak.[211] Thousands of others gathered in other cities around Egypt.[212] These protests criticized the abuses of the police and demanded changes, including the end of emergency law and changes to the term limits of the presidency.[213] On January 26, 2011, the government shut down internet access for most of the country for five days.[214] Protesters continued to find ways to circumvent the government ban and news outlets around the world rushed to find ways to get information about what was happening in Egypt.[215]

---

government demands."); *see also* OPENNET INITIATIVE, *supra* note 104, at 4 (reporting that Vodafone handed over communications data to the Egyptian authorities that may have been used to help identify protesters from the April 2008 strike).

209. *See* Noman, *supra* note 208 (stating that the data may have been used to help identify rioters); *see also* OPENNET INITIATIVE, *supra* note 104, at 4 (explaining how cell phone information was used to help identify participants of the April 2008 protests).

210. *See* Kareem Fahim & Mona El-Naggar, *Across Egypt, Protests Direct Fury at Leader*, N.Y. TIMES, Jan. 26, 2011, at A1 (describing the protests in Egypt); Jennifer Preston, *Movement Began with Outrage and a Facebook Page that Gave It an Outlet*, N.Y. TIMES, Feb. 6, 2011, at A10 (discussing a Facebook group titled "We Are All Khaled Said" that helped spread information about Egyptian abuses and indicating that Khaled Said was an Egyptian who was tortured and killed by Egyptian police).

211. *See* Fahim & El-Naggar, *supra* note 210, at A1 (describing the Egyptian protests); *see also* Ahmir Ahmed, *Thousands Protest in Egypt*, CNN, Jan. 25, 2011, http://articles.cnn.com/2011-01-25/world/egypt.protests_1_street-protests-thousands-protest-economic-policies?_s=PM:WORLD (reporting on the protests).

212. *See* Fahim & El-Naggar, *supra* note 210, at A1 (describing the protests); *see also* Ahmed, *supra* note 211 (providing information regarding the protests).

213. *See* Fahim & El-Naggar, *supra* note 210, at A1 (describing the demands of the protesters); *see also* Ahmed, *supra* note 211 (reporting on the protests).

214. *See* Matt Richtel, *Egypt Halts Most Internet and Cell Service, and Scale of Shutdown Surprises Experts*, N.Y. TIMES, Jan. 29, 2011, at A13 (describing the shutdown as "unprecedented in scope and scale"); *see also* Mark Milian, *Reports Say Egypt Web Shutdown Is Coordinated, Extensive*, CNN (Jan. 28, 2011), http://articles.cnn.com/2011-01-28/tech/egypt.internet.shutdown_1_social-media-egypt-web-instant-messaging?_s=PM:TECH (reporting on the internet shutdown).

215. *See* Richtel, *supra* note 215, at A13 ("Online activists inside and outside the country passed along information about how to work around the shutdown, like using dial-up Internet connections in other countries."); *see also* Christopher Rhoads & Geoffrey A. Fowler, *Egypt Shuts Down Internet, Cellphone Services*, WALL ST. J., Jan. 29, 2011, http://online.wsj.com/article/SB10001424052748703956604576110453371369740.html (describing ways in which activists tried to spread news after the Internet was shut down).

Following weeks of popular protests and pressure, President Hosni Mubarak resigned from office on February 11, 2011.[216] Since then, a military council led by Field Marshal Mohammed Hussein Tantawi, the chairman of the Supreme Council of the Armed Forces, has been exercising interim power.[217] In March 2011, a new constitution was declared.[218]

While the military has promised reform, in September of 2011, the council announced it would continue to enforce the emergency law into 2012.[219] In November, protests began again, this time criticizing the military council's failure to hand over power to an elected group of citizens.[220] Protesters also decried the heavy-handed tactics of the military council in responding to the demonstrations, comparing them to those used during the Mubarak era.[221] After several days of violence and unrest, the civilian cabinet of ministers resigned.[222] The ruling military council agreed to speed up the transition to civilian rule, and

---

216. *See* David D. Kirkpatrick, *Mubarak Out*, N.Y. TIMES, Feb. 12, 2011, at A1 (confirming that Mubarak stepped down from power); Anthony Shadid, *Egyptian Military Dissolves Weak Parliament*, N.Y. TIMES, Feb. 14, 2011, at A1 (explaining the handover of power).

217. *See* Shadid, *supra* note 216, at A1 (detailing the military leaders that took over after President Mubarak stepped down); *see also* David D. Kirpatrick, *Egypt Unclear on Timetable of Power Transfer, U.S. Says*, N.Y. TIMES, Oct. 5, 2011, at A8 (discussing how the military has failed to hand over power to the people).

218. CONSTITUTIONAL DECLARATION OF THE ARAB REPUBLIC OF EGYPT, Mar. 20, 2011, *available at* http://www.egypt.gov.eg/english/laws/constitution/default.aspx; *see* Neil MacFarquhar, *Egypt's Voters Approve Constitutional Changes for Quick Elections*, N.Y. TIMES, Mar. 21, 2011, at A4 (reporting on the new constitution).

219. *See Egyptian Military Institutes New Media Restrictions*, COMMITTEE TO PROTECT JOURNALISTS, (Sept. 13, 2011), http://cpj.org/2011/09/egyptian-military-institutes-new-media-restriction.php (reporting on new media restrictions and confirming that the emergency law remains in effect); *see also* Kirkpatrick, *supra* note 217, at A8 (commenting that the emergency law continues to be in effect and hoping for its end).

220. *See* David D. Kirkpatrick, *Egypt's Cabinet Offers to Resign as Protests Rage*, Nov. 22, 2011, at A1 (describing the new protests in Egypt); *see also* Tamim Elyan & Edmund Blair, *Egyptians Protest at Army, Clashes Kill at Least 12*, REUTERS, Nov. 20, 2011, http://www.reuters.com/article/2011/11/20/us-egypt-protests-idUSTRE7AI0EC20111120 (reporting on the November protests).

221. *See* Kirkpatrick, *supra* note 220, at A1 (describing the tactics of the military in responding to protests); *see also* Elyan & Blair, *supra* note 220 (discussing the reasons why protests occurred again in November).

222. *See* Kirkpatrick, *supra* note 220, at A1 (describing the cabinet's response to the protests); *see also Egypt's Military Accepts Cabinet's Resignation*, CNN (Nov. 22, 2011, 12:53 PM), http://news.blogs.cnn.com/2011/11/22/report-egyptian-officials-reach-deal-on-national-government/ (reporting on the resignation of the cabinet).

elections took place as planned on November 28 and 29, 2011, with Egyptians turning out in large numbers.[223]

While social media may not have been responsible for the revolution in Egypt or its continued repercussions, it has certainly made a significant contribution.[224] The people of Egypt have grasped the possibilities of the medium and have adopted social media norms to effectuate change and demand legitimate reform.[225] In this type of environment, the Egyptian government can no longer avoid making changes.[226]

B. *United Kingdom: The Role of Social Media in the London Riots and the Debate over Super-Injunctions*

There has been a particularly strong clash between the rights of privacy and the freedom of expression in the United Kingdom.[227] The debate has spread to the issuance of super-

---

223. *See* Kirkpatrick, *supra* note 220, at A1 (discussing the planned elections); *see also* Charles Levinson et al., *Egypt's Voters Cast Historic Ballot*, WALL ST. J., Nov. 29, 2011, at A8 (reporting on the Egyptian vote).

224. *See* Fatma Naib, *Online Activism Fuels Egypt Protest*, ALJAZEERA, Jan. 28, 2011, http://www.aljazeera.com/news/middleeast/2011/01/201112810225384873O.html (discussing the influence of social media on the protests); Jillian York, *The Future of Egypt's Internet*, ALJAZEERA (Feb. 1, 2011, 10:45 AM), http://www.aljazeera.com/indepth/opinion/2011/02/20112174317974677.html ("Furthermore, the degree to which online communications were used in Egypt for organising prior to the blackout is simply unprecedented; though electronic communication may not have catalyzed the popular uprising, they certainly helped it along, perhaps even accelerated it.").

225. *See Rumors of a Facebook Block Persist in Egypt*, *supra* note 1 ("There is no freedom of expression and there is no real mass media where we can speak our opinions; so we go to the Internet to speak our opinions with more freedom and increased range." (quoting WaLeed KoraYem, a student in Cairo)); *see also* Preston, *supra* note 210, at A10 ("Facebook, YouTube, Twitter and cellphones made it easy for human rights advocates to get out the news and for people to spread and discuss their outrage . . . in a country where freedom of speech and the right to assemble were limited and the government monitored newspapers and state television.").

226. *See* Kirkpatrick, *supra* note 217, at A1 ("[Mubarak] was toppled by a radically new force in regional politics—a largely secular, nonviolent, youth-led democracy movement that brought Egypt's liberal and Islamist opposition groups together for the first time under its banner."); *see also* David D. Kirkpatrick, *Deal to Hasten Transition Is Jeered at Cairo Protests*, N.Y. TIMES, Nov. 23, 2011, at A1 (discussing how the military council has tried to strike deals with various parts of the political elite, to no avail).

227. *See* Claire Cain Miller & Ravi Somaiya, *Free Speech on Twitter Faces Test*, N.Y. TIMES, May 23, 2011, at B1 (discussing the problems posed by Twitter); *see also* MULLIS & SCOTT, *supra* note 83, at 12–22 (describing problems in the British libel regime).

injunctions by British courts.[228] For example, in May 2011, it was revealed that the UK soccer star Ryan Giggs had obtained a super-injunction to prevent the media from discussing a rumored affair.[229] Twitter users responded by revealing his name on the site.[230] Giggs sued Twitter, attempting to force the company to give him the names of the anonymous users who posted his name.[231] For its part, Twitter has stood firmly by its protection of established internet norms.[232] Analysts have stressed the broad implications of this debate.[233] Privacy protections are vital for individuals involved in a social movement like the Egyptian revolution.[234]

---

228. *See* Miller & Somaiya, *supra* note 227, at B1 (discussing the problem posed by Twitter); *see also* Steven Doughty, *We Will Not Be Gagged, M'lud: As Ryan Giggs Is Named in Parliament as Cheating Star After Weeks of Legal Farce, MPs Launch a Defiant Message*, DAILY MAIL (U.K.), May 24, 2011, http://www.dailymail.co.uk/news/article-1389841/Ryan-Giggs-named-Parliament-cheating-super-injunction-star.html (reporting on the super-injunction controversy).

229. *See* Doughty, *supra* note 228 (reporting on the super-injunction controversy); Sarah Lyall, *Parliament Joins the Fray as Twitter Tests a Law*, N.Y. TIMES, May 24, 2011, at A4 ("The tough ruling banned anyone from reporting his name, her name, the supposed affair, even the very existence of the order itself.").

230. *See* Miller & Somaiya, *supra* note 228, at B1 ("[T]ens of thousands of Internet users have flouted the injunction by revealing his name on Twitter, Facebook and online soccer forums, sites that blur the definition of the press and are virtually impossible to police."); *see also* Lyall, *supra* note 229, at A4 ("The clash between old-media law and new-media reality soon descended into a chaotic farce, with Mr. Giggs's name appearing in some 75,000 postings over the weekend, even as British news organizations were still legally forbidden to print it.").

231. *See* Doughty, *supra* note 228 (reporting on a court order obtained by Giggs demanding that Twitter reveal the identities of the anonymous users who had posted the messages); Lyall, *supra* note 229, at A4 (discussing Ryan Giggs' lawyers' statements that they planned to sue Twitter to find the people behind the initial posts).

232. *See* Miller & Somaiya, *supra* note 227, at B1 (quoting Twitter founder Biz Stone and Twitter general counsel Alex Macgillivray: "Our position on freedom of expression carries with it a mandate to protect our users' right to speak freely and preserve their ability to contest having their private information revealed."); Jillian C. York & Cindy Cohn, *Twitter, Free Speech, Super-Injunctions and the Streisand Effect*, ELECTRONIC FRONTIER FOUND., May 24, 2011, https://www.eff.org/deeplinks/2011/05/twitter-and-free-speech-case-super-injunction (applauding Twitter's policy of notifying its users when the US government demands information about Twitter users).

233. *See* Miller & Somaiya, *supra* note 227, at B1 ("If you step back, that same sort of protection is really vital to have in place when you're talking about the individuals involved in a revolution or a social movement like the Arab Spring." (quoting Thomas R. Burke, chairman of the media law practice at Davis Wright Tremaine)); York & Cohn, *supra* note 232 (stating that super-injunctions are a form of prior censorship and are not permitted under international human rights law).

234. *See* PETER SWIRE, CTR. FOR AM. PROGRESS, SOCIAL NETWORKS, PRIVACY, AND FREEDOM OF ASSOCIATION 1–2 (2011), *available at* http://www.americanprogress.org/

The clash between internet norms, such as privacy and freedom of expression, and the government's desire to rely on a security rationale reached its peak several months after the super-injunction controversy.[235] In early August 2011, several months after the events in Egypt, riots broke out in the United Kingdom after a man was fatally shot by police as they tried to arrest him on suspicion of committing a crime.[236] Rioters used Facebook, Twitter, and BlackBerry Messenger to organize.[237] More than 1900 people were arrested and damages were estimated to be in the hundreds of millions of pounds.[238] During the riots, two London members of Parliament called for a BlackBerry Messenger curfew, proposing a shutdown of the service at certain times of the day.[239]

---

issues/2011/02/pdf/social_networks_privacy.pdf (stressing the importance of privacy protections for people using social media); *see also* OPENNET INITIATIVE, *supra* note 104, at 3 (discussing how bloggers and internet users have been arrested after criticizing the government via social media).

235. *See Riots in Tottenham After Mark Duggan Shooting Protest*, BBC NEWS, Aug. 7, 2011, http://www.bbc.co.uk/news/uk-england-london-14434318 (reporting on the UK riots); *see also* Ravi Somaiya, *London Sees Twin Perils Converging to Fuel Riot*, N.Y. TIMES, Aug. 8, 2011, at A4 (commenting on the underlying causes of the London riots).

236. *See Riots in Tottenham After Mark Duggan Shooting Protest*, *supra* note 235 (describing the source of the protest); *see also* Somaiya, *supra* note 235, at A4 ("The episode in Tottenham began as a small and peaceful march, in which residents gathered outside a police station to protest the killing of a local man, Mark Duggan, in a shooting by police officers last week. Scotland Yard has said that Mr. Duggan . . . was the subject of a 'pre-planned operation' by officers.").

237. *See* John F. Burns & Eric Pfanner, *British Prime Minister Faces Questioning in House of Commons over Rioting*, N.Y. TIMES, Aug. 12, 2011, at A4 (quoting Prime Minister Cameron as stating that the government was working on measures to stop rioters from using social media and that he believed it was "right to stop people communicating via these Web sites and services when we know they are plotting violence, disorder and criminality"); Juliette Garside, *Rioters' Use of Social Media Throws Telecoms Firms into Spotlight*, OBSERVER (U.K.), Aug. 20, 2011, at 37 ("After the overthrow of Hosni Mubarak in Egypt and this summer's looting in England, there is no longer any doubt about the speed with which large crowds can be mobilised on to the streets."). BlackBerry Messenger is an application that allows for instant messaging between users of the BlackBerry phone. *See BBM Features*, BLACKBERRY, http://us.blackberry.com/apps-software/blackberrymessenger/ (last visited May 25, 2012).

238. *See* Laura Smith-Spark, *Britain's Suspected Rioters Face Courts as Order Restored*, CNN (Aug. 12, 2011, 9:19 PM), http://edition.cnn.com/2011/WORLD/europe/08/12/uk.riots/ (detailing the damage that resulted from the UK riots); *see also* James Ball, *London's High Streets Count the Cost of the Riots*, GUARDIAN (U.K.), Aug. 8, 2011, http://www.guardian.co.uk/uk/2011/aug/08/london-riots-cost-retail-business (describing the financial damage done by rioting and looting).

239. *See* Garside, *supra* note 237, at 37 (reporting a proposal by two London members of Parliament calling for a BlackBerry Messenger curfew, shutting down

Afterwards, the police commissioner testified before members of Parliament that the police considered switching off social messaging sites but discovered that they did not have the legal authority to do so.[240] Instead, police accessed encrypted social messaging sites in order to thwart planned riots.[241] After the riots ceased, the government announced plans to review police powers, including those to intervene in mobile communications.[242]

During a special debate on the riots, UK Prime Minister David Cameron told Parliament that "when people are using social media for violence we need to stop them."[243] A week later, Prime Minister Cameron met with the makers of Blackberry, Facebook, and Twitter to discuss ways to limit the use of social media during periods of civil unrest.[244] After being met with charges of hypocrisy and censorship, the prime minister backed off, stating that the government had no intention of restricting internet services, and that the meeting instead would focus on

---

service from 6:00 PM to 6:00 AM); *see also Hackers Deface Blackberry Blog Site over UK Riot Mess*, GMA NEWS ONLINE (Aug. 10, 2011, 10:23 AM), http://www.gmanetwork.com/news/story/228960/scitech/hackers-deface-blackberry-blog-site-over-uk-riot-mess ("Tottenham MP David Lammy was among those calling for the BlackBerry Messenger system (BBM) to be shut down to prevent protesters using it to organize themselves.").

240. *See* Vikram Dodd, *Police Accessed BlackBerry Messages to Thwart Planned Riots*, GUARDIAN (U.K.), Aug. 16, 2011, at 7 (reporting that police had considered switching off social messaging sites); Garside, *supra* note 237, at 37 (explaining that police did not seek authority to close down social media sites).

241. *See* Dodd, *supra* note 240, at 7 ("[Police] were able to use details gained from the seized phones to give officers 'live time monitoring' of BBM and also Twitter."); *see also* Garside, *supra* note 237, at 37 ("Police have already told MPs that they contemplated seeking authority to close down Twitter and other services, but that monitoring communications on these channels allowed them to identify the next targets and send officers to protect the Olympic site, Westfield shopping centre and Oxford Street.").

242. *See* Burns & Pfanner, *supra* note 237, at A4 (discussing the UK government's plans to respond to the riots); Garside, *supra* note 237, at 37 (mentioning the government's plans to meet with social messaging companies).

243. Eric Pfanner, *Cameron Exploring Crackdown on Social Media After Riots*, N.Y. TIMES, Aug. 11, 2011, http://www.nytimes.com/2011/08/12/world/europe/12iht-social12.html (quoting the response by Prime Minister Cameron); *see* Garside, *supra* note 237, at 37 (quoting Prime Minister Cameron).

244. *See* Ravi Somaiya, *In Britain, a Meeting on Limiting Social Media*, N.Y. TIMES, Aug. 26, 2011, at A4 (discussing the results of the meeting); *see also* Josh Halliday, *Government Backs Down on Plan to Shut Down Twitter and Facebook in Crises*, GUARDIAN (U.K.), Aug. 25, 2011, http://www.guardian.co.uk/media/2011/aug/25/government-plan-shut-twitter-facebook (reporting on the meeting).

how law enforcement could better use Twitter and Facebook in emergencies.[245] While some felt that the government and police should be permitted to interfere with communication networks in certain situations, others worried that any "draconian new measures in the [United Kingdom] would undermine the fight for open communication that western democracies championed during the upheavals in the Middle East."[246]

C. *United States: The San Francisco BART Incident, Data Collection Debates, and the Freedom of Speech*

In the wake of the UK riots, problems arose in San Francisco, California, when transit police shot and killed a knife-wielding homeless man on a train platform.[247] Public anger over the shooting sparked protests.[248] Demonstrators stopped trains, in some cases climbing on top of them, and organized their protests by smartphone.[249] Bay Area Rapid Transit ("BART"), the operator of San Francisco's subway, suspended service on its own mobile network for three hours, not allowing passengers to

---

245. *See* Pfanner, *supra* note 243 ("[Cameron's] call for curbs drew protests from free-speech campaigners, saying they were reminiscent of moves by Arab rulers to block digital communications during anti-government uprisings this year."); *see also* Halliday, *supra* note 244 (reporting that human rights groups sent an open letter warning that powers restricting the internet could be susceptible to abuse and undermine free speech).

246. Garside, *supra* note 237, at 37 (criticizing government attempts to shutdown social media and noting that social media had helped government authorities get information and organize clean up); *see* Somaiya, *supra* note 244, at A4 ("Some of the nations that have been criticized by the West for their own draconian crackdowns on inconvenient freedoms of speech have watched Britain's recent struggles with barely disguised glee.").

247. *See* Ned Potter, *BART Protests: San Francisco Transit Cuts Cellphones to Thwart Demonstrators; First Amendment Debate*, ABC NEWS, Aug. 16, 2011, http://abcnews.go.com/Technology/bart-protest-san-francisco-transit-cut-cellphones-prevent/story?id=14311444 (reporting on the Bay Area Rapid Transit ("BART") incident); *see also* Zusha Elinson, *After Cellphone Action, BART Faces Escalating Protests*, N.Y. TIMES, Aug. 20, 2011, at A21 (discussing the BART protests).

248. *See* Potter, *supra* note 247 (reporting on protests after the shooting); *see also* Elinson, *supra* note 247, at A21 ("The incident provoked a series of small protests that drew little attention until Aug. 11, when the transit agency took the unusual step of shutting down cellphone service for several hours as activists prepared for another rally.").

249. *See* Potter, *supra* note 247 (describing the events leading up to BART's actions); *see also* Elinson, *supra* note 247, at A21 (detailing the way in which protestors organized).

make even emergency calls.[250] Early reports indicated that BART asked carriers to turn service off, but subsequent statements by BART stated that staff shut down power and alerted the cell carriers after the fact.[251]

The incident prompted many people to compare BART's suspension of service to the actions taken in Egypt and contemplated in the United Kingdom.[252] Critics have noted that the government may enforce reasonable time, place, and manner restrictions on demonstrations or, in some situations, prevent protests that present a clear and present danger.[253] Transit officials maintained that the actions were necessary to protect public safety and that the transit passengers' right to safety outweighed the rights of freedom of speech and assembly.[254]

The Electronic Frontier Foundation ("EFF") and other groups filed an emergency petition asking the FCC to declare BART's actions a violation of telecom laws, specifically the

---

250. *See* Potter, *supra* note 247 (reporting on the shutdown); *see also* Elinson, *supra* note 247, at A21 ("BART approved the shutdown only after Mr. Wakeman determined that the action was legal under Brandenburg v. Ohio, a Supreme Court decision that lets the government punish speech that incites unlawful activity.").

251. *See* Eva Galperin, *BART Pulls a Mubarak in San Francisco,* ELECTRONIC FRONTIER FOUND. (Aug. 12, 2011), https://www.eff.org/deeplinks/2011/08/bart-pulls-mubarak-san-francisco (commenting on the way BART handled the situation); *see also* Potter, *supra* note 247 (reporting on the incident).

252. *See* Quinn Norton, *BART's Cell-Service Cuts: Not Egypt, But Not Quite America Either,* ATLANTIC, Aug. 26, 2011, http://www.theatlantic.com/technology/archive/2011/08/barts-cell-service-cuts-not-egypt-but-not-quite-america-either/244161/ (comparing BART to the actions of Mubarak); *see also* Galperin, *supra* note 251 (headlining that "BART Pulls a Mubarak in San Francisco").

253. *See, e.g.*, Regan v. Time, Inc., 468 U.S. 641, 648 (1984); Grayned v. City of Rockford, 408 U.S. 104, 115 (1972); Cox v. New Hampshire, 312 U.S. 569, 576 (1941); *see also* Megan Delockery, *BART's Cell Phone Shutdown: Protection of Public Safety or Infringement of Constitutional Rights?,* JETLAW: VAND. J. ENT. & TECH. L. (Aug. 23, 2011), http://www.jetlaw.org/?p=7623 ("The ACLU noted that the government may enforce reasonable time, place, and manner restrictions on demonstrations or, in some situations, prevent protests that present a clear and present danger.").

254. *See* Delockery, *supra* note 253 ("BART officials claimed 'that they had the right to [disrupt cell phone service] because it is illegal to protest on trains, train platforms, and outside of designated areas inside the stations.'"); *see also* Elinson, *supra* note 247, at A21 ("BART approved the shutdown only after Mr. Wakeman determined that the action was legal under Brandenburg v. Ohio, a Supreme Court decision that lets the government punish speech that incites unlawful activity.").

Communications Act of 1934.[255] According to the EFF, BART has proposed a new policy for use in future incidents that clarified the extremely limited circumstances under which BART may shut down service.[256] The EFF provided feedback and in December 2011, BART released its new policy.[257] The FCC responded with a statement commending BART for taking steps to adopt a new policy and stating that the FCC would soon announce an "open, public process to provide guidance on these issues."[258]

General concerns over violations of the Fourth Amendment persist as government agencies continue to seek information from ISPs.[259] In 2007, telecommunications giant Verizon informed Congress that it received over 90,000 requests for customer data from law enforcement agencies each year.[260] In

---

255. *See* Emergency Petition in the Matter of the Petition of Public Knowledge et al. for Declaratory Ruling that Disconnection of Telecommunications Services Violates the Communications Act (Fed. Commc'ns Comm'n Aug. 29, 2011), *available at* http://www.publicknowledge.org/files/docs/publicinterestpetitionFCCBART.pdf [hereinafter Emergency Petition for Declaratory Ruling]. The Electronic Frontier Foundation ("EFF") is nonprofit organization founded in 1990 with the aim of confronting issues regarding privacy, free speech, innovation, and consumer rights. *About EFF*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/about (last visited May 25, 2012).

256. *See* PROPOSED CELL SERVICE INTERRUPTION POLICY, BAY AREA RAPID TRANSIT (BART) (Oct. 19, 2011), *available at* http://www.bart.gov/docs/BART_Cell_Interruption_Policy.pdf (presenting a draft of a new cell phone interruption proposal).

257. *See* Trevor Timm, *BART Board Members Pledge to Implement Many of EFF's Recommendations in Their Cell Phone Policy*, ELECTRONIC FRONTIER FOUND. (Oct. 30, 2011), https://www.eff.org/deeplinks/2011/10/bart-board-members-pledge-implement-many-eff's-recommendations-their-cell-phone (detailing the EFF's recommendations); *see also* BAY AREA RAPID TRANSIT, CELL SERVICE INTERRUPTION POLICY (2011), *available at* http://www.bart.gov/docs/final_csip.pdf (presenting the final version of BART's new cell phone interruption policy); Eva Galperin, *BART Considers a Cell Phone Shutdown Policy*, ELECTRONIC FRONTIER FOUND. (Oct. 26, 2011), https://www.eff.org/deeplinks/2011/10/bart-considers-cell-phone-shutdown-policy (welcoming BART's new policy).

258. Press Release, Fed. Commc'ns Comm'n, FCC Chairman Julius Genachowski's Statement on BART Policy Adoption (Dec. 1, 2011), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2011/db1201/DOC-311310A1.pdf.

259. *See* Angwin, *supra* note 57, at A1 (detailing recent clashes between ISPs and government authorities); Helft & Miller, *supra* note 58, at A1 (reporting on the large number of information requests made by government authorities).

260. *See* Angwin, *supra* note 57, at A1 (describing the information requests made by government authorities); Helft & Miller, *supra* note 57, at A1 ("Verizon told Congress in 2007 that it received some 90,000 such requests each year.").

2009, Facebook stated that subpoenas and other orders were arriving at the company at a rate of ten to twenty a day.[261] In the first half of 2010, Google counted more than 4200 of such customer data requests.[262] This legal pressure has resulted in companies like Facebook, Google, and Twitter finding themselves on the front lines of the war between government's security considerations and Fourth Amendment concerns.[263] The possibilities of social media have proven to be extremely tempting for law enforcement agencies.[264] Groups have struggled to keep these government agencies at bay while waiting for the law to catch up with technology.[265]

In January 2012, the online community reacted strongly and swiftly to news of the Stop Online Piracy Act ("SOPA"), a proposed bill that aimed to combat copyright infringement.[266] Together with its counterpart, the Protect IP Act ("PIPA"), the bill would restrict access to sites that host or facilitate the trading of pirated material.[267] SOPA would potentially hold the

---

261. *See* Helft & Miller, *supra* note 57, at A1 ("Facebook told *Newsweek* in 2009 that subpoenas and other orders were arriving at the company at a rate of 10 to 20 a day."). *See generally* Angwin, *supra* note 57, at A1 (discussing the information requests made to sites such as Facebook).

262. *See* Helft & Miller, *supra* note 57, at A1 ("Concerned by the wave of requests for customer data from law enforcement agencies, Google last year set up an online tool showing the frequency of these requests in various countries. In the first half of 2010, it counted more than 4,200 in the United States."). *See generally* Angwin, *supra* note 57, at A1 (describing legal problems that have arisen between ISPs and government authorities).

263. *See* Angwin, *supra* note 57, at A1 (discussing the issues that have arisen as government agencies continue to make information requests); Cohen, *supra* note 69, at B3 (describing Twitter's response to information requests); Helft & Miller, *supra* note 57, at A1 (reporting on the large number of information requests made by government authorities).

264. *See* Angwin, *supra* note 57, at A1 (explaining how law enforcement agencies have used social media); Cohen, *supra* note 69, at B3 (detailing the way that Twitter has responded to government requests for information); Helft & Miller, *supra* note 57, at A1 (discussing the large amount of requests for information made by law enforcement authorities).

265. *See* Emergency Petition for Declaratory Ruling, *supra* note 255 (showing how groups try to keep governmental authorities in check); *see also* Angwin, *supra* note 57, at A1 (detailing recent clashes between ISPs and government authorities).

266. Stop Online Piracy Act (SOPA), H.R. 3261, 112th Cong. (2012); *see* Julianne Pepitone, *SOPA Explained: What It Is and Why It Matters*, CNN MONEY (Jan. 20, 2012, 12:44 PM), http://money.cnn.com/2012/01/17/technology/sopa_explained/index.htm (introducing the Stop Online Piracy Act ("SOPA").

267. PROTECT IP Act (PIPA), S.968, H.R. 3261, 112th Cong. (2011); *see* Pepitone, *supra* note 266 (describing SOPA and the Protect IP Act ("PIPA")).

operators of websites such as YouTube responsible for the content that their users upload.[268] Critics of SOPA and PIPA stated that the bills were poorly written and would effectively promote censorship.[269] On January 18, 2012, popular internet sites such as Wikipedia and Reddit shut down service for twenty-four hours in protest, stating that the legislation was at odds with freedom of speech rights and urging supporters to contact their representatives.[270] By the end of the day, several members of Congress had withdrawn their support from the bills.[271] Once expected to quickly pass, SOPA and PIPA were effectively grounded on January 20, 2012, when congressional leaders postponed the vote, effectively shelving the bills.[272]

Initial development of the Internet led to the adoption of specific internet norms and standards by international organizations, engineering groups, and governmental agencies.[273] In particular, freedom of expression and privacy were norms that historically guided regulation of the Internet.[274] As the Internet has spread, governments have struggled to react to the growth of social media, leading to clashes between

---

268. *See* Pepitone, *supra* note 266 (discussing the potential problems with SOPA); John D. Sutter, *Why Wikipedia Went Down at Midnight*, CNN (Jan. 18, 2012, 4:59 PM), http://www.cnn.com/2012/01/17/tech/web/wikipedia-sopa-blackout-qa/index.html?hpt=hp_c1 (presenting an overview of the problems that websites had with SOPA).

269. *See* Pepitone, *supra* note 266 ("[O]pponents say that the way SOPA is written effectively promotes censorship and is rife with the potential for unintended consequences."); *see also* Jonathan Weisman, *Antipiracy Bills Delayed After an Online Firestorm*, N.Y. TIMES, Jan. 21, 2012, at B6 (reporting on the problems posed by SOPA).

270. *See* Pepitone, *supra* note 266 (describing Wikipedia's protest); *see also* Jonathan Weisman, *Web Rises up to Deflect Bills Seen as Threat*, N.Y. TIMES, Jan. 19, 2012, at A1 (explaining the success of Wikipedia's approach to protesting SOPA and PIPA).

271. *See* Pepitone, *supra* note 266 (discussing the results of protest over SOPA); *see also* Weisman, *supra* note 270, at A1 (reporting on members of Congress who withdrew their support for the bills in the face of widespread criticism of the bill).

272. *See* Weisman, *supra* note 270, at A1 (reporting on the results of internet protests); *see also* Eric Morath & Geoffrey Fowler, *Congress Tosses Antipiracy Bills*, WALL ST. J., Jan. 21, 2012, http://online.wsj.com/article/SB10001424052970204301404577172703397383034.html (discussing the postponement of the votes on SOPA and PIPA).

273. *See supra* Part I.2 (discussing the technological groups, international organizations, and governmental agencies that created and adopted internet norms and standards).

274. *See supra* Part I.2 (describing the ways in which technological groups, international organizations, and governmental agencies adopted privacy and freedom of expression as internet norms).

governments and established internet norms.[275] The Egyptian revolution of early 2011 showed how people around the world have the expectation that internet norms such as freedom of expression will be respected, even if it is not a traditional norm of the state.[276] The UK riots of August 2011 and the recent development of the super-injunction illustrated the problems governments face when trying to reconcile their own laws with technological realities and the expectations of the international community.[277] Finally, San Francisco's shutdown of mobile service in August 2011, and concerns over the collection and storage of personal data by the authorities in the United States, demonstrates that the difficulties governments face when trying to regulate social media are universal, and that a security rationale is not a persuasive rationale when interfering with social media.[278]

III. *GOVERNMENTS MUST RESPECT ESTABLISHED INTERNET NORMS WHEN REGULATING SOCIAL MEDIA*

Governments must respect established internet norms such as freedom of expression and privacy when attempting to regulate social media. This Note argues that the security rationale used by governments is not persuasive, as freedom of expression and privacy concerns have consistently trumped security considerations since the dawn of the Internet, especially in the American context. While the rise of social media may have amplified security concerns, the US government should remain true to its initial objectives when formulating policy. This Note concludes that rather than implementing policies that interfere with social media as security threats arise, as in the BART incident, the US government should try to craft policies and legislation that work *with* the Internet.

---

275. *See supra* Part II.A (explaining recent clashes between the government and established Internet norms in Egypt, the United Kingdom, and the United States).

276. *See supra* notes 210–16 and accompanying text (describing the role that social media played in the Egyptian revolution).

277. *See supra* notes 231–46 (discussing recent clashes in the United Kingdom).

278. *See supra* notes 252–65 and accompanying text (describing debates over the BART incident and data collection policies in the United States).

As the Internet has become a pervasive part of peoples' lives, governments have been forced to adapt quickly.[279] Governments around the world have struggled with responding to new technology and have yet to establish a clear approach to dealing with the capabilities of social media.[280] As a result, governments have taken a haphazard approach, dealing with situations as they arise.[281] In some cases, this has lead to disastrous results.[282] When responding to incidents, international governments have used a security rationale, explaining that interference in social media is necessary to preserve public safety.[283] The short history of the Internet, however, has demonstrated that the security rationale is not persuasive.[284] While the initial architects of the Internet were concerned with network security and the structural integrity of the Internet, this concern did not extend to physical safety and security.[285] Security, in the sense that governments attempt to use it, is not an accepted internet norm.[286] Therefore,

---

279. *See, e.g.*, *supra* notes 214–15 and accompanying text (describing the Egyptian government's response to mass protests); *supra* notes 241–42 and accompanying text (discussing the United Kingdom's attempt to shut down mobile service during riots); *supra* notes 255–58 and accompanying text (explaining how groups in the US responded to the BART incident).

280. *See, e.g.*, *supra* notes 216–17 and accompanying text (discussing the Egyptian government's response to demonstrations); *supra* notes 241–44 and accompanying text (describing the United Kingdom's contemplation of a mobile service shutdown); *supra* notes 250–51 and accompanying text (explaining BART's reaction to demonstrations).

281. *See, e.g.*, *supra* notes 214–15 and accompanying text (describing how the Egyptian government dealt with mass protests); *supra* notes 241–42 and accompanying text (discussing the United Kingdom's attempt to shut down mobile service during riots); *supra* notes 250–51 and accompanying text (explaining how BART responded to demonstrations).

282. *See supra* notes 211–16 and accompanying text (discussing the Egyptian revolution).

283. *See supra* note 214 and accompanying text (explaining that the Egyptian government shut down the Internet using a security rationale); *supra* notes 243–46 and accompanying text (noting that the British government had contemplated shutting down the Internet in the future in the interest of safety); *supra* note 254 and accompanying text (discussing BART's assertion that their shutdown of cell service was valid under a security-based understanding).

284. *See supra* notes 186–95 and accompanying text (asserting that technological groups and international organizations refer to network security and not physical security as an established internet norm).

285. *See supra* notes 186–95 and accompanying text (discussing how the initial architects of the Internet approached security questions).

286. *See supra* notes 186–95 and accompanying text (describing the way in which technological and engineering groups discuss security).

government attempts to rationalize internet interference as a valid exercise of their police power will necessarily fail.[287]

As this Note has illustrated, in confrontations with internet-related matters, internet norms have begun to trump traditional government norms.[288] While certain countries may hold vastly different political and social values, the democratic character and nature of the Internet has resulted in the expectation of certain rights, regardless of international boundaries or borders.[289] When governments try to assert their superiority, they have been met with opposition, and were forced to either retreat and lose face or take action and risk reaction.[290]

Of the three countries discussed in this Note, Egypt is the most extreme example of this phenomenon.[291] Egypt was a totalitarian state whose ruler was in power for thirty years.[292] While Egypt had a democratic constitution, the imposition of emergency law curtailed most human rights.[293] Freedom of expression and privacy were not established as governmental norms of the Egyptian state.[294] Yet, as internet use became more

---

287. *See supra* notes 210–15 and accompanying text (discussing the response to the Egyptian government's move to shut down the Internet); *supra* notes 247–50 and accompanying text (noting the criticism that erupted after Prime Minister Cameron stated that in some cases social media regulation was warranted); *supra* notes 255–58 and accompanying text (describing the response to BART's shutdown of mobile service in San Francisco).

288. *See supra* notes 225–26 and accompanying text (discussing Egypt as an example of a country where internet norms have trumped government norms).

289. *See supra* notes 225–26 and accompanying text (using Egypt as an example when explaining that people around the world have begun to expect that internet norms will be respected, even if they are not traditional values found in their countries).

290. *See supra* notes 210–16 and accompanying text (describing how President Mubarak was forced to step down after weeks of protest); *supra* notes 245–46 and accompanying text (discussing Prime Minister Cameron's response to criticism after proposing social media restrictions); *supra* notes 255–58 and accompanying text (mentioning the response to BART's shutdown of mobile service in San Francisco).

291. *See supra* notes 216–18 and accompanying text (discussing the overthrow of the Egyptian government and the establishment of a new constitution).

292. *See supra* notes 200–10 and accompanying text (presenting a background of policies formed under the rule of former President Hosni Mubarak).

293. *See supra* notes 199–201 and accompanying text (describing the curtailment of many rights under emergency law in Egypt under the rule of former President Hosni Mubarak).

294. *See supra* note 197 and accompanying text (noting that Egypt never respected traditionally Western values such as freedom of expression and privacy).

prevalent, these principles became expected.[295] For example, the Egyptian youth developed expectations of privacy in their homes.[296] They also demanded the right to be able to express themselves, criticize the government, and demand change.[297] When an authoritarian state takes aggressive actions to control its opponents it is a sign that the regime believes it faces a threat.[298] The Egyptian government tried to exert control in the way it had for the past three decades and discovered it could no longer do so.[299] Unable to match the diffusive power of the Internet and social media sites, the government reacted by shutting them down.[300] This prohibitive action did not quell the riots, however, and actually had the effect of inflaming them.[301]

While the United Kingdom has a more established tradition of freedom of expression and privacy rights compared to Egypt, the understanding of these rights is very different than that in the United States.[302] The United Kingdom also has experienced a clash of norms in recent months.[303] After 9/11, the United Kingdom tightened security and increased surveillance measures, relying heavily on a security rationale to justify their actions.[304] Critics of the UK government's approach have called it the realization of a "Big Brother" society.[305] At the same time, the country supported the events that occurred in Egypt and

---

295. *See supra* notes 202–05 and accompanying text (discussing Egyptians' expectations of respect for internet norms).

296. *See supra* notes 202–05 and accompanying text (discussing the way internet norms became expected by Egyptian citizens using the Internet).

297. *See supra* notes 202–05 and accompanying text (discussing the ways in which Egyptians came to expect internet norms).

298. *See supra* notes 206–14 and accompanying text (asserting that the Egyptian governments' response signaled its fear and confusion towards the Internet).

299. *See supra* notes 206–16 and accompanying text (discussing the Egyptian government's response to protests and the subsequent overthrow of Hosni Mubarak).

300. *See supra* note 214 and accompanying text (tracing the government's reaction to the protests).

301. *See supra* notes 216–18 and accompanying text (discussing the overthrow of the Egyptian government and the establishment of a new constitution).

302. *See supra* notes 84–88 and accompanying text (describing the different understanding of certain rights in the United Kingdom).

303. *See supra* note 227 and accompanying text (introducing recent problems Britain has faced).

304. *See supra* notes 93–94 and accompanying text (discussing new measures adopted by the British government).

305. *See supra* note 95 and accompanying text (noting criticisms of the current surveillance regime in the United Kingdom).

other Middle Eastern nations during the "Arab Spring."[306] Consequently, the UK government faced charges of hypocrisy after it contemplated restricting access to services during the riots in August 2011.[307] In addition, the flaws in the libel regime of the United Kingdom have resulted in a haphazard approach to governance.[308] The common law has been distorted as a result of the lack of clear principles and now it must be addressed.[309] This Note contends that the United Kingdom should look to established internet norms and standards in determining its policy going forward. The confusing and often contradictory laws of the nation are no longer reconcilable with the realities of the Internet. Like Egypt, the United Kingdom must adapt to new technology and the expectations that come with it.

The United States also has found itself in this precarious position.[310] Freedom of expression and privacy are two constitutional principles engrained in the American consciousness.[311] As a result, any interference with those rights has been met not only with social but legal questions.[312] The public's response to SOPA and the subsequent reaction of Congress is illustrative of the power of these norms.[313] The US government is no longer able to unilaterally define the parameters of norms such as freedom of speech and privacy.[314]

---

306. *See supra* note 245 and accompanying text (mentioning that the UK government was criticized for proposing to adopt the same measures adopted by the Egyptian government).

307. *See supra* notes 245–46 and accompanying text (noting criticism of the UK government's calls to regulate social media).

308. *See supra* notes 89–92 and accompanying text (discussing the problems in the British libel regime and noting the need for reform).

309. *See supra* notes 89–92 and accompanying text (noting the issues in British libel regime).

310. *See supra* notes 246–52 and accompanying text (discussing the BART shutdown of cell service in San Francisco).

311. *See supra* Part I.A.1 and accompanying text (presenting the constitutional underpinnings of the rights of freedom to expression and privacy).

312. *See supra* notes 44–53 and accompanying text (explaining first amendment issues concerning internet regulation); *supra* notes 58–78 and accompanying text (describing Fourth Amendment issues and illustrating their application to internet regulations).

313. *See supra* notes 266–72 and accompanying text (describing the successful initiative undertaken by the public to prevent SOPA from being passed).

314. *See supra* notes 266–72 and accompanying text (discussing how the public successfully relied on internet norms in opposing SOPA).

Instead, the process has become truly democratic, as people are able to shape the norms themselves.[315]

This Note recommends that the US government should respect internet norms when crafting legislation and policy. This approach would be the most reconcilable with American jurisprudence and also would help resolve the ongoing First and Fourth Amendment issues. [316] The Supreme Court has established that the government cannot restrict expression because of its message, ideas, subject matter, or content.[317] While there are exceptions where the government may use time, place, and manner regulations to further significant governmental interests, groups have continuously challenged government attempts to regulate the Internet on First Amendment grounds.[318] Any government attempts to regulate social media sites using a security rationale (claiming, for example, that it is likely to incite imminent violence or will lead reasonable people to fear violence) would similarly be criticized and challenged. On the other hand, the internet community would likely embrace an approach that favored transparency, openness, and full disclosure.

Government intervention poses a greater threat to free speech than private action. At this point in time, the government should act with restraint to prevent regulation that could have unintended and farreaching consequences. The US government should favor self-regulation approaches for the Internet, with minimal or transparent government intervention. Private intermediaries have played a vital role in internet governance and should continue to do so in the future.[319] International groups, such as the WGIG, economic groups, such as the OECD, and engineering groups, such as the IETF, all

---

315. *See supra* notes 266–72 and accompanying text (explaining how the public's opposition to SOPA was effective in helping to overcome it).

316. *See supra* notes 71–74 and accompanying text (discussing an example of the ways US courts have approached these kinds of constitutional questions).

317. *See supra* notes 45–47 and accompanying text (discussing the First Amendment as it relates to internet regulation).

318. *See supra* notes 47–53 and accompanying text (noting First Amendment challenges that were made concerning legislation which sought to regulate internet content).

319. *See supra* notes 54–57 and accompanying text (discussing the importance of Section 230 of the CDA in encouraging private action).

possess expertise in the field.[320] They are therefore better equipped than the government to deal with many of the common issues that arise because they understand and respect users' expectations. Putting regulation in the hands of intermediaries allows multiple groups to work together to determine their mutual best interests, solving problems that the government is simply unable to solve.[321] These groups add inherent legitimacy to any actions taken and thus are best suited to regulate the Internet when necessary.

The US government also should amend the ECPA to reflect the current realities of communication on the Internet, using established internet norms as a guide. While the US Supreme Court has yet to decide whether a person has a reasonable expectation of privacy in their e-mail, the public has clearly decided that communication over the Internet is here to stay.[322] As e-mail and messaging services increasingly replace physical mail, interest in their protection has increased accordingly.[323] Meanwhile, the US government makes more and more requests for information on individuals from ISPs such as Google.[324] While some surveillance measures may be necessary for national security, any internet regulation should be aimed at protecting user privacy rather than expanding the government's power.[325] Internet privacy principles support the contention that a substantial revision to the ECPA is warranted.[326]

---

320. *See supra* notes 138–43, 165–72 and accompanying text (describing the different organizations and the roles that they play in internet governance).

321. *See supra* notes 147–48 and accompanying text (noting the importance of technological organizations in developing the rules for network regulation).

322. *See supra* notes 71–74 and accompanying text (describing federal court cases that have recently been decided concerning a person's right to privacy in his or her e-mail); *supra* notes 76–77 and accompanying text (describing legislation pending in Congress that seeks to update the laws that relate to internet technology).

323. *See supra* notes 71–74 and accompanying text (describing federal court cases that have recently been decided concerning a person's right to privacy in his or her e-mail).

324. *See supra* notes 261–67 and accompanying text (discussing the increasing number of requests for personal information made by government authorities and the legal implications of these requests).

325. *See supra* notes 177–86 and accompanying text (explaining how certain internet norms and standards have emerged and have been adopted and asserting that these norms are those that should be respected by governments).

326. *See supra* notes 63–70 and accompanying text (criticizing the ECPA); *supra* notes 263–69 and accompanying text (discussing the need for reform concerning personal data collection by government authorities).

Until the law is able to catch up to technology, the US government must tread lightly as it tries to determine its appropriate role and the best way for it to protect the public. This Note concludes that the government should look to established internet norms such as openness, transparency, and innovation when dealing with internet issues rather than relying on a security rationale. This approach is consistent with existing American jurisprudence and statutes.[327] Additionally, the US government should look at users' expectations regarding the established norms and standards. Fortunately, many third parties already have systems in place to protect these principles.[328] The Internet provides a way for governments to achieve many of their goals.[329] These governments must, however, understand that they are now required to play by the Internet's rules. The time when a government could impose norms and principles without incurring a public reaction is past.

CONCLUSION

Internet norms and standards have become accepted by users around the world. As social media use has become pervasive, people have grown to expect that certain norms will be respected. For example, the people of Egypt used social media sites to spread news, discuss their political opinions, and organize protests. Although the freedoms of expression and privacy have never been traditionally accepted norms of the Egyptian state, the people demanded the acceptance of these norms. Similarly, there was outrage in the United Kingdom and the United States after government officials threatened to shut down social media.

Governments, in turn, have responded with a security rationale, arguing that they have the authority to act to protect

---

327. *See supra* notes 43–52, 57–59 and accompanying text (describing the protections of the US Constitution).

328. *See supra* notes 135–37 and accompanying text (discussing the ways that technological and engineering groups established principles and standards); *supra* notes 151–54 (introducing the way international organizations use the norms of freedom of expression, privacy, and transparency when formulating Internet governance guidelines); *supra* notes 177–81 and accompanying text (describing how governmental agencies in the United States have adopted these norms).

329. *See supra* notes 69–70 and accompanying text (discussing ways law enforcement agencies use information found on social media sites).

the public. Government authorities also have attempted to argue that security is an established internet norm that it is trying to protect. Recent events have proven this argument to be unpersuasive. While governments may have authority to act to protect public safety, they must be careful to avoid excessive responses. When attempting to regulate social media, the government must act within accepted internet norms and standards in order to maintain legitimacy in its actions.