FREEDOM OF ASSOCIATION IN A NETWORKED WORLD: FIRST AMENDMENT REGULATION OF RELATIONAL SURVEILLANCE

KATHERINE J. STRANDBURG*

Abstract: Recent controversies about the National Security Agency's warrantless wiretapping of international calls have overshadowed equally disturbing allegations that the government has acquired access to a huge database of domestic call traffic data, revealing information about times, dates, and numbers called. Although communication content traditionally has been the primary focus of concern about overreaching government surveillance, law enforcement officials are increasingly interested in using sophisticated computer analysis of noncontent traffic data to "map" networks of associations. Despite the rising importance of digitally mediated association, current Fourth Amendment and statutory schemes provide only weak checks on government. The potential to chill association through overreaching relational surveillance is great. This Article argues that the First Amendment's freedom of association guarantees can and do provide a proper framework for regulating relational surveillance and suggests how these guarantees might apply to particular forms of analysis of traffic data.

INTRODUCTION

The National Security Agency (the "NSA") has reportedly obtained a vast database of telephone records from some of the major

 Visiting Associate Professor of Law, New York University School of Law; Associate Professor of Law, DePaul University College of Law. A short report of this work has been published as Katherine J. Strandburg, *Surveillance of Emergent Associations: Freedom of Association in a Network Society*, *in* DIGITAL PRIVACY: THEORY, TECHNOLOGIES AND PRACTICES (Alessandro Acquisti et al. eds., 2007). I am grateful for comments on this project from Michael Birnhack; Niva Elkin-Koren; Peter Swire; Diane Zimmerman; participants in the Center for Discrete Mathematics and Theoretical Computer Science Workshop on Information Security Economics at Rutgers University (January 18–19, 2007); participants in the Haifa University Research Seminar on Law, Society, and Technology; and participants in a faculty workshop at DePaul University College of Law. I am also grateful to DePaul's University Research Council for a Faculty Leave Research Grant, which supported part of this work. Excellent research assistance from Elizabeth Levine is also gratefully acknowledged.

telephone companies.[1] There are continuing efforts to require Internet service providers ("ISPs") to maintain records of their customers' travels over the Internet.[2] The European Union has already adopted a controversial Directive mandating telecommunications traffic data retention.[3] Popular attention has been focused intensely on "warrantless wiretapping" of the *content* of communications in light of continuing revelations about the Bush administration's post-September 11, 2001 surveillance programs and controversy over legislation intended to regulate that surveillance and to immunize telecommunications from liability for their participation.[4] The surveillance efforts that are the focus of this Article, however, make use of the endpoints of communications, so-called "traffic data," rather than their con-

---

[1] *See* Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls: 3 Telecoms Help Government Collect Billions of Domestic Records*, USA TODAY, May 11, 2006, at A1; Barton Gellman & Arshad Mohammed, *Data on Phone Calls Monitored: Extent of Administration's Domestic Surveillance Decried in Both Parties*, WASH. POST, May 12, 2006, at A1. Recent reports suggest that the NSA has cast an even broader net for traffic data than even that alleged in the earlier reports concerning telephone call records. *See* Siobhan Gorman, *NSA's Domestic Spying Grows as Agency Sweeps Up Data*, WALL ST. J., March 10, 2008, at A1.

[2] *See, e.g.*, Wendy R. Liebowitz, *Call for Uniform Data Retention Standards for ISPs to Help in Child Porn Investigations*, 5 Privacy & Security L. Rep. (BNA) No. 27, at 935 (July 3, 2006); Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951, 973 (2006); *Virginia Panel Urges One Year ISP Data Retention*, 6 Privacy & Security L. Rep. (BNA) No. 1, at 26 (Jan. 1, 2007) [hereinafter *Virginia Panel Urges*]; Saul Hansell & Eric Lichtblau, *U.S. Wants Internet Companies to Keep Web-Surfing Records*, N.Y. TIMES, June 2, 2006, at A15.

[3] European Parliament and Council Directive 2006/24, 2006 O.J. (L 105) 54, 57 (EC); *see also European Union Officials Formally Approve Data Retention Plan for Phone Calls, E-Mails*, 5 Privacy & Security L. Rep. (BNA) No. 9, at 275 (Feb. 27, 2006) [hereinafter *European Union Officials*]. Countries do have some flexibility in how the Directive is implemented. *See, e.g.*, Arthur Rogers, *U.K. Adopts Telecom Data Retention Law, Exempts Internet Communications*, 6 Privacy & Security L. Rep. (BNA) No. 32, at 1247 (Aug. 6, 2007).

[4] *See, e.g.*, Alexei Alexis, *Feingold Declares War on Surveillance Bill Approved by Senate Intelligence Committee*, Privacy L. Watch (BNA) (Oct. 22, 2007) [hereinafter Alexis, *Feingold Declares War*]; Alexei Alexis, *FISA Legislation Pulled from House Floor as Republicans Propose Set-Back Measure*, Privacy L. Watch (BNA) (Oct. 18, 2007) [hereinafter Alexis, *FISA Legislation Pulled*]; Alexei Alexis, *House Commerce Turns to Administration for Details on Alleged Telecom Data-Sharing*, Privacy L. Watch (BNA) (Oct. 16, 2007) [hereinafter Alexis, *House Commerce Turns to Administration*]; Alexei Alexis, *House Judiciary, Intel Panels Reject Legislation to Provide Telecom Immunity*, Privacy L. Watch (BNA) (Oct. 11, 2007) [hereinafter Alexis, *House Judiciary, Intel Panels Reject Legislation*]; Alexei Alexis, *Hoyer: Informal FISA Talks So Far Yield No Deal on Telecom Immunity*, Privacy L. Watch (BNA) (Feb. 27, 2008); Alexei Alexis, *Surveillance Program Broader than Previously Reported, McConnell Says*, Privacy L. Watch (BNA) (Aug. 3, 2007); Eric Lichtblau, *Court Weighs Making Public Rulings on U.S. Wiretapping*, N.Y. TIMES, Aug. 18, 2007, at A10; Eric Lichtblau, *Role of Telecom Firms in Wiretaps Is Confirmed*, N.Y. TIMES, Aug. 24, 2007, at A13; Ralph Lindeman, *Senate Panel Delays Action on FISA Bill: Markup Could Be Pushed into December*, Privacy L. Watch (BNA) (Nov. 9, 2007); James Risen, *Bush Signs Law to Widen Reach for Wiretapping*, N.Y. TIMES, Aug. 6, 2007, at A1.

tents.[5] Attempts to use such noncontent information about communications to ferret out suspect groups and investigate their membership and structure are increasingly in vogue, but have yet to receive the attention from legal scholars and policy makers that they deserve.[6] Traffic analysis is being updated to incorporate insights from "social network analysis"—a means of analyzing relational structures originally developed by sociologists—and to take advantage of the avail-

---

[5] *See generally* George Danezis, *Introducing Traffic Analysis: Attacks, Defences and Public Policy Issues . . . (Invited Talk)*, http://homes.esat.kuleuven.be/~gdanezis/TAIntro.pdf (last visited Mar. 3, 2008) (providing an explanation of traffic analysis).

[6] There are, on the other hand, numerous articles and studies discussing the Fourth Amendment implications of data mining of transactional information and the Internet's effect on surveillance of communications content. *See generally* KIRSTIE BALL ET AL., SURVEILLANCE STUDIES NETWORK, A REPORT ON THE SURVEILLANCE SOCIETY (David Murakami Wood ed., 2006); DAVID COLE & JAMES X. DEMPSEY, TERRORISM AND THE CONSTITUTION (3d ed. 2006); STEPHEN J. SCHULHOFER, THE ENEMY WITHIN (2002); DANIEL J. SOLOVE, THE DIGITAL PERSON (2004); Patricia Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375 (2004); Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6 (2003); Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241 (2007); Joseph S. Fulda, *Data Mining and Privacy*, 11 ALB. L.J. SCI. & TECH. 105 (2000); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975 (2007); Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373 (2006) [hereinafter Henderson, *Learning from All Fifty States*]; Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2006); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004) [hereinafter Kerr, *Constitutional Myths*]; Seth F. Kreimer, *Watching the Watchers: Surveillance, Transparency, and Political Freedom in the War on Terror*, 7 U. PA. J. CONST. L. 133 (2004); Paul Rosenzweig, *Civil Liberty and the Response to Terrorism*, 42 DUQ. L. REV. 663 (2004); Paul Rosenzweig, *Privacy and Consequences: Legal and Policy Structures for Implementing New Counter-Terrorism Technologies and Protecting Civil Liberty*, *in* EMERGENT INFORMATION TECHNOLOGIES AND ENABLING POLICIES FOR COUNTER-TERRORISM 421 (Robert L. Popp & John Yen eds., 2006) [hereinafter EMERGENT INFORMATION TECHNOLOGIES]; Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. (forthcoming 2008) [hereinafter Slobogin, *Government Data Mining*], *available at* http://ssrn.com/abstract=1001972; Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139 (2005) [hereinafter Slobogin, *Transaction Surveillance*]; Daniel J. Steinbock, *Data Matching, Data Mining, and Due Process*, 40 GA. L. REV. 1 (2005); Katherine J. Strandburg, *Social Norms, Self Control, and Privacy in the Online World*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION 31 (Katherine J. Strandburg & Daniela Stan Raicu eds., 2006); Peter P. Swire, Katz *Is Dead. Long Live* Katz, 102 MICH. L. REV. 904 (2004) [hereinafter Swire, Katz *Is Dead*]; Swire, *supra* note 2; K.A. Taipale, *Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance*, 7 N.Y.U. REV. L. & SECURITY, No. VII Supplemental Bull. on L. & Security (2006), *available at* http://whisperingwires.info; Joseph T. Thai, *Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?*, 74 FORDHAM L. REV. 1731 (2006); Jonathan Zittrain, *Searches and Seizures in a Networked World*, 119 HARV. L. REV. F. 83 (2006), http://www.harvardlawreview.org/forum/issues/119/dec05/zittrainfor05.pdf.

ability of computational techniques for mining vast databases of traffic information.[7] Although "relational surveillance" making use of traffic data has been around for many years, recent social and technological developments have combined to raise the stakes.[8] Current legal doctrine, which centers on "privacy" and hence on protecting the content of communications, does not adequately account for the extent to which relational surveillance threatens to chill expressive association in today's networked world. Courts have yet even to consider the First Amendment implications of relational surveillance of this type.[9]

---

[7] *See generally* Albert-László Barabási, Linked: The New Science of Networks (2002); T. Kolda et al., Sandia Nat'l Labs. & Lawrence Livermore Nat'l Lab., Data Sciences Technology for Homeland Security Information Management and Knowledge Discovery (2004); Jeffery W. Seifert, Congressional Research Serv., Data Mining: An Overview, (2004), *available at* http://www.fas.org/irp/crs/RL31798.pdf; Duncan J. Watts, Six Degrees: The Science of a Connected Age (2003); Kathleen M. Carley et al., *Destabilizing Networks*, 24 Connections 79 (2001), *available at* http://www.insna.org/Connections-Web/Volume24-3/Carley.web.pdf; Peter Klerks, *The Network Paradigm Applied to Criminal Organisations: Theoretical Nitpicking or a Relevant Doctrine for Investigations? Recent Developments in the Netherlands*, 24 Connections 53 (2001), *available at* http://www.insna.org/Connections-Web/Volume24-3/Klerks.web.pdf; Robert L. Popp et al., *Utilizing Information and Social Science Technology to Understand and Counter the Twenty-First Century Strategic Threat*, *in* Emergent Information Technologies, *supra* note 6, at 1; Karl M. van Meter, *Terrorists/Liberators: Researching and Dealing with Adversary Social Networks*, 24 Connections 66 (2001), *available at* http://www.insna.org/Connections-Web/Volume24-3/Karl.van.Meter.web.pdf; Stanley Wasserman et al., *Introduction* to Models and Methods in Social Network Analysis 1 (Peter J. Carrington et al. eds., 2005); Patrick Radden Keefe, *Can Network Theory Thwart Terrorists?*, N.Y. Times, Mar. 12, 2006, § 6 (Magazine), at 16; Nasrullah Memon & Henrik Legind Larsen, Practical Approaches for Analysis, Visualization and Destabilizing Terrorist Networks (2006) (on file with author); Danezis, *supra* note 5; George Danezis & Bettina Wittneben, The Economics of Mass Surveillance and the Questionable Value of Anonymous Communications, http://weis2006.econinfosec.org/docs/36.pdf (last visited Mar. 9, 2008); Sofus A. Macskassy & Foster Provost, Suspicion Scoring Based on Guilt-By-Association, Collective Inference, and Focused Data Access (2005), https://analysis.mitre.org/proceedings/Final_Papers_Files/273_Camera_Ready_Paper.pdf. For a discussion of the relevance of network analysis to law more generally, see Katherine J. Strandburg et al., *Law and the Science of Networks: An Overview and an Application to the "Patent Explosion,"* 21 Berkeley Tech. L.J. 1293, 1310–18 (2006).

[8] *See* Klerks, *supra* note 7, at 56–58; van Meter, *supra* note 7, at 67–70; Danezis, *supra* note 5, § 2.

[9] I argue in this Article that the First Amendment's protection of freedom of association should play a key role in regulating relational surveillance. Two other scholars have also argued in important recent articles that the First Amendment has a critical role to play in regulating surveillance, but have emphasized the First Amendment's free speech aspects. *See generally* Matthew Lynch, *Closing the Orwellian Loophole: The Present Constitutionality of Big Brother and the Potential for a First Amendment Cure*, 5 First Amendment L. Rev. 234 (2007) (arguing, after rejecting other approaches as inadequate, that pervasive Orwellian surveillance is unconstitutional under the First Amendment as a restriction on a speaker's right to choose her audience and hence to choose not to speak to the government); Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. Rev. 112 (2007). I agree with their emphasis on the First Amendment implications of surveillance but focus

Digital technology has transformed the ways in which civic and political associations are formed and operate.[10] Nearly every organization now uses email, websites, and cellular phones as primary means of communications with members. Meanwhile, more and more political and civic "work" in society is performed not by traditionally organized, relatively long-lived, face-to-face associations with well-defined members, leaders, policies, and goals, but by decentralized, often transient, networks of individuals associating only or primarily electronically and with policies and goals defined synergistically with the formation of the emergent association itself. Relational surveillance has great potential to chill this increasingly important emergent association, particularly for those who are members of, or associate with members of, religious and political minority groups. Fears of being swept up mistakenly in the broad and vague applicability of statutes such as the criminal prohibition on "material support" of a designated terrorist organization or of

---

here more specifically on the issue of freedom of association in a networked society because I believe both that its importance is underappreciated and that freedom of association doctrine is poised to play an important part in the debate because of its recent strong endorsement by the Supreme Court in the case of *Boy Scouts of America v. Dale*. *See* 530 U.S. 640, 655–56 (2000). Solove briefly discusses the freedom of association implications of surveillance. *See* Solove, *supra*, at 147–49. Lynch sees "hope" in freedom of association doctrine as a means of regulating pervasive Orwellian surveillance but, in the end, prefers an argument based on the right to choose one's audience. *See* Lynch, *supra*, at 260–64. My focus here is different. I am concerned about the threat to association posed by sophisticated analysis of traffic data, not by the equally important issue of government "listening in" on the content of speech.

[10] For some of the numerous discussions of this topic, see generally Yochai Benkler, The Wealth of Networks: How Social Production Transforms Markets and Freedom (2006); Howard Rheingold, Smart Mobs: The Next Social Revolution (2002); Diana Saco, Cybering Democracy: Public Space and the Internet (2002); Julie Cohen, *Cyberspace as/and Space*, 107 Colum. L. Rev. 210 (2007); Michael J. Madison, *Social Software, Groups, and Governance*, 2006 Mich. St. L. Rev. 153; Martha McCauhey & Michael D. Ayers, *Introduction* to Cyberactivism: Online Activism in Theory and Practice 1 (Martha McCauhey & Michael D. Ayers eds., 2003) [hereinafter Cyberactivism]; Douglas Schuler & Peter Day, *Shaping the Network Society: Opportunities and Challenges*, *in* Shaping the Network Society: The New Role of Civil Society in Cyberspace 1 (Douglas Schuler & Peter Day eds., 2004); Peter M. Shane, *Introduction: The Prospects for Electronic Democracy*, *in* Democracy Online: The Prospects for Political Renewal Through the Internet, at xi (Peter M. Shane ed., 2004); Wim van de Donk et al., *Introduction: Social Movements and ICTs*, *in* Cyberprotest: New Media, Citizens and Social Movements 1 (Wim van de Donk et al. eds., 2004) [hereinafter Cyberprotest]; Anupam Chander, *Whose Republic?*, 69 U. Chi. L. Rev. 1479 (2002) (reviewing Cass Sunstein, Republic.com (2001)); Beth Simone Noveck, *A Democracy of Groups*, First Monday, Nov. 7, 2005, http://firstmonday.org/issues/issue10_11/noveck.

being placed on a "no-fly" list no doubt heighten the chilling effect likely to flow from increasing use of relational surveillance.[11]

Interest in employing social network analysis for law enforcement purposes began with the study of criminal organizations,[12] but was given a huge boost after September 11, 2001, when attention focused on tracking terrorist networks.[13] The focus on preventing terrorism rather than investigating past crimes, along with the tendency for terrorist groups to be organized in decentralized networks of "cells" rather than traditional hierarchies, has brought relational surveillance to the center of the law enforcement agenda.[14] At the same time, rising use of the Internet, wireless communication, and locational technology means that traffic data is increasingly recorded and stored by third party intermediaries. Computational capabilities have also increased dramatically in the past few years, making it possible to apply computerized analysis to larger datasets and heightening law enforcement and counterterrorism interest in employing data mining techniques to uncover "suspicious" patterns of association in traffic data.[15]

---

[11] *See* 18 U.S.C.A. §§ 2339A–2339B (West 2000 & Supp. 2007); *see, e.g.*, David Cole, *The New McCarthyism: Repeating History in the War on Terrorism*, 38 Harv. C.R.-C.L. L. Rev. 1, 1–2 (2003); Nina J. Crimm, *High Alert: The Government's War on the Financing of Terrorism and Its Implications for Donors, Domestic Charitable Organizations, and Global Philanthropy*, 45 Wm. & Mary L. Rev. 1341, 1404–19 (2004); Linda E. Fisher, *Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups*, 46 Ariz. L. Rev. 621, 625, 662 n.224 (2004); Randolph N. Jonakait, *The Mens Rea for the Crime of Providing Material Resources to a Foreign Terrorist Organization*, 56 Baylor L. Rev. 861, 869–72 (2004); Kreimer, *supra* note 6, at 165–69; Tom Stacy, *The "Material Support" Offense: The Use of Strict Liability in the War Against Terror*, 14 Kan. J.L. & Pub. Pol'y 461, 462–63 (2005); Kathryn A. Ruff, Note, *Scared to Donate: An Examination of the Effects of Designating Muslim Charities as Terrorist Organizations on the First Amendment Rights of Muslim Donors*, 9 N.Y.U. J. Legis. & Pub. Pol'y 447, 471–75 (2005); Stephen Townley, Note, *The Hydraulics of Fighting Terrorism*, 29 Hamline L. Rev. 65, 66–68 (2006); *ACLU Faults Terrorism Screening System for Detention, Harassment of U.S. Travelers*, Privacy L. Watch (BNA) (June 27, 2006); Joyce E. Cutler, *Civil Rights Group Seeks Watch List Details in FOIA Lawsuit Against Treasury Department*, Privacy L. Watch (BNA) (May 23, 2007); Leslie Eaton, *U.S. Prosecution of Muslim Group Ends in Mistrial*, N.Y. Times, Oct. 23, 2007, at A1; Eric Lichtblau, *F.B.I. Scrutinizes Antiwar Rallies*, N.Y. Times, Nov. 23, 2003, at A1; Neil MacFarquhar, *Abandon Stereotypes, Muslims in America Say*, N.Y. Times, Sept. 4, 2007, at A12.

[12] *See* Klerks, *supra* note 7, at 54–56.

[13] *See* Taipale, *supra* note 6; van Meter, *supra* note 7, at 74; Gellman & Mohammed, *supra* note 1; Keefe, *supra* note 7; Memon & Larsen, *supra* note 7, § 1; Danezis, *supra* note 5, § 3.

[14] *See* Cole & Dempsey, *supra* note 6, at 19; Kolda et al., *supra* note 7, at 1; Schulhofer, *supra* note 6, at 1; Klerks, *supra* note 7, at 53–57; van Meter, *supra* note 7, at 74–76; Memon & Larsen, *supra* note 7, § 1.

[15] *See, e.g.*, Seth A. Greenblatt et al., *Behavioral Network Analysis for Terrorist Detection*, *in* Emergent Information Technologies, *supra* note 6, at 331, 332–33; van Meter, *supra* note 7, at 70–73; Keefe, *supra* note 7.

Historically, both constitutional and statutory protections of communications from government surveillance have been strongest for the content of the communications, with significantly decreased protection for traffic data, which reveals who is talking to whom.[16] Viewed through the paradigm of secrecy and individual privacy that has dominated the jurisprudence of surveillance under the Fourth Amendment, this sliding scale of protection makes sense. Wiretapping a telephone seems more intrusive than obtaining a list of the numbers an individual has dialed, and the privacy invasion associated with government attention to the content of a conversation seems correspondingly greater than the harm of revealing the mere fact that the conversation occurred.

The growing potential for wide-reaching relational surveillance, however, challenges the notion that the harm caused by unfettered government surveillance is necessarily commensurate with the amount of communication content revealed. Though considerable literature has developed around the threat to privacy posed by aggregation and categorization of personal information about specific individuals,[17] there has as yet been little discussion of the particular implications of relational surveillance as a distinctive type of government intrusion. Computerized analysis of relationship networks is less widely publicized and less fully developed than data mining techniques used to build "digital dossiers" about individuals.[18] Traffic data, however, when stored, aggregated, and analyzed using sophisticated computer algorithms, contains far more "information" than is commonly appreciated.[19] It is time for serious consideration of the appropriate means for Congress and the courts to regulate relational surveillance.

Current law does not adequately contend with relational surveillance, particularly in view of the increasing importance of emergent association. Fourth Amendment doctrine and statutory privacy protections, with their focus on the content of communications, provide very limited protection of traffic data and transactional records.[20] The potential chilling effect due to relational surveillance poses serious risks not only to individual privacy, but to the First Amendment rights to freedom of association and assembly. This is an important distinc-

---

[16] *See* Slobogin, *Transaction Surveillance*, *supra* note 6, at 149, 152.

[17] *See, e.g.*, SOLOVE, *supra* note 6, at 1–10; Slobogin, *Transaction Surveillance*, *supra* note 6, at 139–40 (citing sources).

[18] *See* SOLOVE, *supra* note 6, at 1–26 (discussing data mining techniques used to build "digital dossiers" about individuals).

[19] *See* Danezis, *supra* note 5, § 1.

[20] *See infra* notes 121–207 and accompanying text.

tion because, although Fourth Amendment doctrine is grounded in a perspective of "reasonable expectations" of privacy and hence has a majoritarian bent, the First Amendment protects unpopular and even "unreasonable" expression.[21] The main contention of this Article is that First Amendment freedom of association guarantees must provide an additional check, distinct from the Fourth Amendment's protections from unreasonable search and seizure, on overreaching relational surveillance potential.[22] Freedom of association case law, however, as exemplified by the U.S. Supreme Court's decision in 2000, in *Boy Scouts of America v. Dale*, has so far been concerned with the rights of existing, formal associations and has not yet adapted to the networked world.[23] The doctrine must be adapted to apply to the forms of association that define today's important political and cultural milieu. As this Article argues in detail below, the First Amendment's freedom of association guarantees require that any program of relational surveillance meet a strict scrutiny standard.[24] The surveillance must serve a legitimate and compelling government interest and its methodology must be sufficiently accurate and narrowly tai-

---

[21] *See* United States v. Playboy Entm't Group, Inc., 529 U.S. 803, 816–17 (2000); Katz v. United States, 389 U.S. 347, 353, 357–58 (1967) (establishing reasonable expectation of privacy test for Fourth Amendment). This distinction has some relevance to the ongoing debate as to whether the courts or the legislative branch are best suited to regulate government surveillance. *See, e.g.*, Kerr, *Constitutional Myths*, *supra* note 6, at 858 (arguing that Congress is best suited to regulate surveillance using new technologies); Swire, Katz *is Dead*, *supra* note 6, at 905 (arguing that courts have an important role to play in regulating surveillance using new technologies). Courts may be uniquely sensitive to the important protection of minority expressive association even if legislatures are more attuned to mean "reasonable expectations of privacy."

[22] *See infra* notes 276–353 and accompanying text.

[23] *See* 530 U.S. at 648, 655–56. In *Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups*, Linda E. Fisher considers the impact of surveillance on the freedom of association of political and religious groups and argues that the expansive protection of groups' expressive freedom should limit political surveillance, but her article focuses on real space surveillance. Fisher, *supra* note 11, at 643–45. In *Watching the Watchers: Surveillance, Transparency, and Political Freedom in the War on Terror*, Seth F. Kreimer argues that freedom of association is threatened by loose interpretations of criminal prohibitions on "material support" to terrorists. Kreimer, *supra* note 6, at 165. For the most part, however, scholarly consideration of freedom of association has debated the role of traditional civic associations in today's world but has yet to grapple extensively with new forms of association facilitated by cyberspace or with the relationship between free association and surveillance. *See generally* Civil Society and Government (Nancy L. Rosenblum & Robert C. Post eds., 2002); Nancy L. Rosenblum, Membership and Morals: The Personal Uses of Pluralism in America (1998); Daniel A. Farber, *Speaking in the First Person Plural: Expressive Associations and the First Amendment*, 85 Minn. L. Rev. 1483 (2001); David Bernstein, *Expressive Association After* Dale, Soc. Phil. & Pol'y, July 2004, at 195.

[24] *See infra* notes 208–275 and accompanying text.

lored to that interest in light of the extent to which it is likely to expose protected expressive and intimate associations. Although it will be quite possible to meet this standard in many instances involving law enforcement and counterterrorism, the standard must be enforced. Because current law imposes only the most minimal restrictions on government access to and analysis of traffic data, current standards are far from meeting this constitutional requirement.[25]

Part I of this Article explores the increasing importance for social and political life of "emergent associations" that make use of modern digital communication technology.[26] Part II discusses the increasing availability of traffic data.[27] It then introduces the concept of social network analysis, explaining (and speculating to some extent about) the ways in which traffic data might be used for surveillance and discussing some of the pitfalls of such uses.[28] Part III discusses the relevant legal frameworks for protecting emergent associational life, focusing on the Fourth Amendment/statutory surveillance law paradigm and on First Amendment protection of freedom of association.[29] Although concluding that the First Amendment right to freedom of association provides the strongest basis for regulating relational surveillance, it extracts suggestive principles from Fourth Amendment doctrine about how surveillance regulation must respond to technological change. These principles can be employed to extend the First Amendment analysis into the new age of electronic communications. Part IV sets out a framework for analyzing relational surveillance programs and makes an initial attempt to apply this freedom of association framework to some specific types of relational surveillance.[30]

I. Relational Surveillance and Networks of Association

New communication technologies are opening up exciting new possibilities for civil and political association. The Internet, embodied in the World Wide Web, email, listserves, chat rooms, weblogs, and instant messaging, has revolutionized the organization of grassroots political movements.[31] The speed and asynchronous nature of Internet

---

[25] *See infra* notes 171–207 and accompanying text.

[26] *See infra* notes 31–36 and accompanying text.

[27] *See infra* notes 37–58 and accompanying text.

[28] *See infra* notes 59–116 and accompanying text.

[29] *See infra* notes 117–275 and accompanying text.

[30] *See infra* notes 276–379 and accompanying text.

[31] *See, e.g.*, Arthur Edwards, *The Dutch Women's Movement Online: Internet and the Organizational Infrastructure of a Social Movement*, *in* Cyberprotest, *supra* note 10, at 183, 191–200

communication makes it an ideal tool for rapidly mobilizing a group of like-minded citizens. The Internet also facilitates broad-based recruiting through web pages and listserves and, perhaps even more importantly, harnesses the high connectivity and information advantages of social networks because of the ease of email forwarding and hyperlinking. These features allow political and civic associations to organize and adapt quickly without necessarily using a central command and control strategy.[32] Newer technologies, combining Internet communication with locational information, promise even more.[33]

Today's emergent associations differ in important ways from traditional political and social organizations because digital communication technology has lowered the costs of collective activity and decreased the importance of geographical proximity. Associations can emerge on all size scales and can be geographically local or dispersed. They can form around very specific issues and then die out quickly. They may remain loosely connected and dispersed or eventually coalesce into more traditional forms of organization with paid staff, hierarchical organization, centralized decision making, and so forth. Strategies, issues, and positions can either be selected using a specified democratic process or imposed by a central leadership; or an association may self-organize out of the independent actions of individuals. Expressive associations can quickly "piggyback" on existing social networks or organizational affiliations. A bicycle club, for example, may be instantly transformed by its listserve into an advocacy group when local ordinances related to bicycle traffic or funding for bike lanes are up for consideration. Such a group need not adopt an official stance on an issue in order to produce a compelling presence at a city council meeting or a flood of emails to an elected official. The low cost (both financial and otherwise) of starting and participating in collective behavior using modern communication technology facilitates experimentation by individuals and by

---

(examining uses of the Internet by several grassroots organizations in the Dutch women's movement); Joanne Lebert, *Wiring Human Rights Activism: Amnesty International and the Challenges of Information and Communication Technologies*, *in* CYBERACTIVISM, *supra* note 10, at 209, 210–23 (examining Amnesty International's use of information and communication technologies, including email and the Internet, for information production/dissemination and grassroots communication, coordination, and mobilization efforts).

[32] *See* RHEINGOLD, *supra* note 10, at 157–58 (providing examples of the use of "smart mob" behavior and "swarming" tactics for group mobilization through various methods of Internet communication, including email, text messaging, and webcasts of digital video); Timothy Zick, *Clouds, Cameras, and Computers: The First Amendment and Networked Public Places*, 59 FLA. L. REV. 1, 18–19 (2007); Noveck, *supra* note 10.

[33] *See, e.g.*, RHEINGOLD, *supra* note 10, at xi–xxii; Zick, *supra* note 32, at 18–21.

groups. It allows groups to reconfigure quickly to address social issues as they arise. The network structure permits established groups to join together quickly and easily for particular actions, while remaining separate for others, and many-to-many communication facilitates cooperation between different groups.

These features of emergent association are exciting and promising for a number of reasons. Although money is never absent as a feature of political life, inexpensive Internet communication opens the door to a more effective exercise of political power by groups without significant material resources. It also permits the faster and more effective aggregation of financial resources from many individuals to serve as an alternative to more traditional fundraising, which must focus on the well-heeled. The anonymity (or, more accurately, pseudonymity) of Internet communication also facilitates the emergence of groups that might never otherwise have formed because potential members might have been deterred from participating until the involvement of a threshold number of others was assured.

The characteristics of modern communications technology that enhance association, however, also enhance the potential that association will be chilled by relational surveillance. Although the threads of Internet organization and other digital communication are invisible in the physical world, they can be all too easily traced in cyberspace. This will be all the more true if ISPs are required to retain logs of Internet transactions. Not only can surveillance of emergent associations be more complete because of their cyberspace "tracks" but, as discussed in Part II, network analysis has at least the potential to expose these associations to government or public scrutiny at a much earlier stage of organization than would be possible for a traditional, "real space" organization.[34] Long before there is a name for the association, a platform of positions, slate of officers, or membership list (indeed an emergent association may sometimes accomplish its purpose without ever having any of those things), the associational pattern is recorded in the traffic data. Associations may be evident from communication patterns even before the participants themselves are aware that they have formed a collective enterprise and certainly before participants have made the kind of intentional "joining" decision that is typical for traditional organizations.

For these emergent associations, and even for traditional associations that make extensive use of digital communications, the potential

---

[34] *See infra* notes 37–116 and accompanying text.

chilling effects of relational surveillance are profound. Not only might the tracing of patterns of communications be essentially equivalent to exposing (and thereby chilling) knowing membership in an unpopular group, but the mining of association from communication patterns also exposes exploratory activities, such as inquiries, participation in email campaigns, or subscribing to an informational listserve, which could mark an individual as a "member" of an association before any "joining" decision has been made. Moreover, as discussed below, computational techniques for analyzing social networks are far from perfect and can categorize an individual as a member of a group simply because he or she has some other connection to some of its members.[35] Because the complete network of relations is not apparent to participants, the only way to ensure that one is not mistakenly associated with an unpopular group is to confine one's communications to those well within the mainstream. Relational surveillance, even more than government investigation of membership in traditional associations, has the potential to chill not only knowing association with unpopular groups, but even the exploration of nonmainstream ideas in a social context. Comprehensive relational surveillance (or even the appearance or threat of comprehensive relational surveillance) has the unfortunate propensity to nip in the bud the very types of informal and flexible associations that modern technology has just begun to produce.

Of course, like all advances in communication technology, the Internet and related digital communication technologies are useful not only to legitimate political and civic groups but also to criminal and terrorist groups. These organizations can also benefit from the pseudonymity and loose structure of emergent association. Indeed, fear that digital communication technology may enhance the effectiveness of malevolent associations drives government and law enforcement efforts in relational surveillance. The difficult policy question is how to regulate relational surveillance so that it can be used by the authorities when and if appropriate, but not abused or used at too great a cost to liberty. Unfortunately, as will be discussed in Part III, the current legal regime, both statutory and constitutional, has yet even to acknowledge, let alone to account for, the importance of emergent association and the danger of relational surveillance.[36]

---

[35] *See infra* notes 59–116 and accompanying text.

[36] *See infra* notes 117–275 and accompanying text.

II. The Rise in Relational Surveillance

In May 2006, newspaper headlines were full of reports that the NSA had been secretly amassing a huge database of phone call records obtained from many of the country's leading telephone companies.[37] Subsequent news reports have suggested that the government's use of the call records database produced intense controversy among Department of Justice lawyers in 2004.[38] This revelation, following on the heels of earlier revelations of NSA warrantless wiretapping of international phone calls, produced widespread concern about government overreaching. The Bush administration eventually agreed to submit its warrantless wiretapping program to review by the specialized court set up by the Foreign Intelligence Surveillance Act ("FISA"), but complained that the resulting rulings, which have not been made public, were too restrictive.[39] Congress eventually bowed to White House pressure, passing highly controversial legislation, which expanded government wiretapping authority in some circumstances for a six month period, after which the issue was to be reconsidered by Congress.[40] That legislation was allowed to expire and debate continues as to the eventual scope of foreign intelligence wiretapping powers.[41]

Though news reports commonly lump the two NSA programs together, they appear to be distinct: the government contends that the

---

[37] *See, e.g.*, Cauley, *supra* note 1; Gellman & Mohammed, *supra* note 1; *see also* Gorman, *supra* note1 (providing further reports concerning government use of even more extensive databases of transactional data).

[38] Scott Shane & David Johnston, *Mining of Data Prompted Fight over U.S. Spying*, N.Y. Times, July 29, 2007, at A1.

[39] Eric Lichtblau et al., *Reported Drop in Surveillance Spurred a Law*, N.Y. Times, Aug. 11, 2007, at A1; Eric Lichtblau & David Johnston, *Court to Oversee U.S. Wiretapping in Terror Cases*, N.Y. Times, Jan. 18, 2007, at A1. That court issued orders, which have not been made public, regulating the program. Lichtblau & Johnston, *supra*, at A1. The American Civil Liberties Union filed a lawsuit seeking disclosure of the orders, which was denied. Dan Eggen, *Secret Court Asks for White House View on Inquiry: ACLU Seeking Rulings Issued on Warrantless Wiretapping*, Wash. Post, Aug. 18, 2007, at A3; Elizabeth Williamson, *Secret U.S. Intelligence Court Intends to Keep Wiretap Rulings Under Wraps*, Wash. Post, Dec. 12, 2007, at A27.

[40] *See* Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (2007) (codified as amended as amended at 50 U.S.C.A. §§ 1801–1805c (West 2003 & Supp. II 2007)); Lichtblau et al., *supra* note 39; James Risen, *Bush Signs Law to Widen Reach for Wiretapping*, N.Y. Times, Aug. 6, 2007, at A1; James Risen & Eric Lichtblau, *Concerns Raised on Wider Spying Under New Law*, N.Y. Times, Aug. 19, 2007, at A1.

[41] *See* Alexei Alexis, *Bush Vows to Veto House "Compromise" on FISA as Democrats Allow Secret Session*, Privacy L. Watch (BNA) (Mar. 14, 2008) [hereinafter Alexis, *Bush Vows*]; Alexei Alexis, *House Commerce Democrats Renew Call for Warrantless Wiretapping Details*, Privacy L. Watch (BNA) (Mar. 10, 2008).

warrantless wiretapping is aimed at scanning the content of international calls to and from "potential terrorists," but the reported aim of the database of phone call records (which, as far as one can tell, includes millions of purely domestic calls) is to facilitate "network analysis" presumably for purposes of relational surveillance.[42] The NSA's programs are the subject of the Electronic Frontier Foundation's lawsuit against AT&T.[43] The suit alleges that AT&T broke the law when it provided the government access both to call content and to its phone call records database.[44] The lawsuit is currently before the U.S. Court of Appeals for the Ninth Circuit.[45] The government is seeking to have the suit dismissed on national security grounds.[46] Congress is also considering controversial provisions in the new surveillance legislation that would immunize the telecommunications companies from liability for their complicity in the NSA programs, with the House and Senate having passed competing bills.[47]

A. *The Availability of Traffic Data*

The publicity surrounding the NSA allegations and lawsuits dramatically highlights the extent to which telephone traffic data is routinely recorded and stored by commercial carriers, in part for billing purposes.[48] ISPs are another repository of large caches of traffic data. ISP logs contain traffic data about email senders and recipients, instant message participation, participation in chat rooms, and also records of Internet "surfing," which can be used to track the online behavior of particular individuals.[49] Although ISPs generally do not bill on a per-transaction basis and need not save their logs of Internet traffic for very

---

[42] *See, e.g.*, Cauley, *supra* note 1; Keefe, *supra* note 7.

[43] *See* Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 978–80 (N.D. Cal. 2006).

[44] *Id.*

[45] *See* Hepting v. AT&T Corp., Nos. 06-17132, 06-17137 (9th Cir. argued Aug. 15, 2007).

[46] Reply Brief for the United States at 2, *Hepting*, Nos. 06-17132, 06-17137 (9th Cir. May 2007). For updated information about the status of the lawsuit, see Electronic Frontier Foundation, www.eff.org (last visited Mar. 4, 2008).

[47] *See* Alexis, *Bush Vows*, *supra* note 41; Bob Egelko, *Feinstein Backs Legal Immunity for Telecom Firms in Wiretap Cases*, S.F. Chron., Nov. 9, 2007, at B1; Eric Lichtblau, *House Votes to Reject Immunity for Phone Companies Involved in Wiretaps*, N.Y. Times, Mar. 15, 2008, at A13; Eric Lichtblau, *In Wiretap Law's Stead, Uncertainty*, N.Y. Times, Feb. 27, 2008, at A17; Eric Lichtblau, *In Senate, a White House Victory on Eavesdropping*, N.Y. Times, Jan. 25, 2008, at A19; Jonathan Weisman & Ellen Nakashima, *Senate and Bush Agree on Terms of Spying Bill*, Wash. Post, Oct. 18, 2007, at A1. *Compare* S. 2248, 110th Cong. (2007), *with* H.R. 3773, 110th Cong. (2008).

[48] *See supra* notes 37–47 and accompanying text.

[49] *See* Solove, *supra* note 6, at 167–68.

long, many do save detailed logs of Internet traffic for purposes ranging from troubleshooting to marketing.[50] Some ISPs claim that they intentionally destroy those logs to protect the anonymity and confidentiality of their customers.[51] Indeed, recent controversy over Google's use of search query records have led Microsoft and Ask.com to announce, presumably in an attempt to attract privacy-conscious users, that they will take steps to curtail the amount of personal log information they maintain.[52] Law enforcement officials, however, would like to ensure the expanded availability of Internet traffic logs for many reasons.[53] Partly in response to concerns about child pornography, the European Union recently passed a Data Retention Directive requiring ISPs to maintain logs for law enforcement purposes for a certain period of time.[54] Similar proposals to require retention of traffic data have been floated in the U.S. Congress, though none has yet been passed.[55]

Telephone call records and ISP logs are only the tip of the iceberg of traffic data that could be made available to the government. Financial records, for example, are also a source of relational information. There have been complaints internationally that certain companies that handle large numbers of financial transactions have made their records available to the U.S. government in contravention of local privacy laws.[56] As more phone calls are made from wireless phones (and emails more often are sent between mobile, wireless devices) it becomes increasingly possible to maintain records not only of calling numbers, call recipients, and call times, but also of the geographical locations of call-

---

[50] Alexei Alexis, *FTC to Examine Consumer Tracking Practices Used by Online Ad Industry*, Privacy L. Watch (BNA) (Aug. 7, 2007); Saul Hansell, *Advertisers Trace Paths Users Leave on Internet*, N.Y. Times, Aug. 15, 2006, at C1.

[51] Miguel Helft, *Ask.com Puts a Bet on Privacy*, N.Y. Times, Dec. 11, 2007, at C1.

[52] *Id.*; *see also* Alexei Alexis, *Competition Could Help Reform Online Ad Industry, Report Says*, Privacy L. Watch (BNA) (Aug. 9, 2007).

[53] *See* Solove, *supra* note 6, at 166.

[54] *See* European Parliament and Council Directive 2006/24, 2006 O.J. (L 105) 54, 57 (EC); *European Union Officials*, *supra* note 3, at 275; Rogers, *supra* note 3, at 1247.

[55] *See* Liebowitz, *supra* note 2, at 935; *Virginia Panel Urges*, *supra* note 2, at 26; Hansell & Lichtblau, *supra* note 2.

[56] *See, e.g.*, Joe Kirwin, *EU Data Privacy Officials Say U.S.-SWIFT Deal Breaches Law, Seek Halt to U.S. Data Access*, 5 Privacy & Security L. Rep. (BNA) No. 47, at 1657 (Dec. 4, 2006). This particular controversy is being resolved by changes to the agreement about data exchanges. Rick Mitchell, *SWIFT Joins U.S. Safe Harbor, Allowing EU Data Transfers for U.S. Anti-Terror Probes*, 6 Privacy & Security L. Rep. (BNA) No. 31, at 1210 (July 30, 2007); Rick Mitchell, *SWIFT Plans Changes to Assuage Concerns over Privacy, Expects Safe Harbor Approval*, 6 Privacy & Security L. Rep. (BNA) No. 29, at 1124 (July 16, 2007).

ers and recipients.[57] Location may be inferred from the locations of the call towers which carried the calls or obtained from precise geographical tracking data associated with GPS technology employed to facilitate emergency response or, more trivially, to provide locationally cued services such as restaurant reviews or "yellow pages" services.[58]

The exploding availability of traffic data on communications is not the result of any Big Brother program of surveillance. It is a natural byproduct of modern communication technologies, social practices that rely increasingly on communication carried by commercial intermediaries, and the fact that technology for data storage has improved to the point that it is extremely cheap to keep records and to store them—indeed probably cheaper simply to keep everything than to figure out what to keep and what to destroy. These trends can only be expected to continue. Unless they are precluded from doing so by law or public pressure, commercial intermediaries will sell—or simply provide—communication traffic data to the government. The era when most communications and associations were shielded by practical obscurity and faded into history is over. Citizens and policymakers must grapple with the question of how a nearly comprehensive record of the network of private communications should be regulated and used.

B. *Evolving Uses of Traffic Data and Social Network Analysis*

The use of traffic data for law enforcement and by the military has a long history.[59] For example, in World War I, military officials analyzed the earth returns of telegraph communications near transmitting stations to obtain traffic information about telegraph communications.[60] When the military began to rely on wireless communications, these communications were tracked and intercepted.[61] Even when the content of the communications was unavailable because, for example, it was encrypted, the traffic data was analyzed.[62] The analysis of communications networks also has a relatively long history.[63] In 1941, for example, such data was used by the British to reconstruct the network

---

[57] *See* Rheingold, *supra* note 10, at 97–100; van Meter, *supra* note 7, at 71–72; Danezis, *supra* note 5, § 4.

[58] *See* Rheingold, *supra* note 10, at 97–100.

[59] *See* Danezis, *supra* note 5, § 2.

[60] *Id.*

[61] *Id.*

[62] *See id.*

[63] *See id.*

structure of the German Air Force, thus allowing a more accurate estimate of German military strength.[64]

These historical precursors, however, differ from today's uses of traffic data in both kind and degree. Historically, the use of traffic data was limited both by the need to intercept traffic data in real time (and hence to know in advance what data to intercept) and by the difficulty in analyzing such data using "pen and paper" techniques.[65] The extent to which traffic data is automatically recorded today means that there is no technological need to identify the subjects of relational surveillance in advance. Because nearly all communications are conducted through intermediaries whose records can in principle be obtained retrospectively, relational surveillance is not constrained by practical limitations on the number of communications that can be tracked. Advanced computational capability combines with the availability of such complete records to change the nature of relational surveillance profoundly. Not only is it possible to map out the immediate associates of a target individual, but the network of associations may be extended to the associates of those immediate associates and so forth.

Social network analysis provides a variety of metrics for comparing different social networks and for analyzing the positions of particular individuals in the network.[66] For example, an individual's role in the network can be measured in terms of "degree" (the number of associations the individual has) or "betweenness" (the extent to which relationships between other members of the network go "through" a particular individual).[67] The network itself can be characterized, among other things, by its degree of reciprocity (the extent to which relationships "go both ways"—I call you and you call me—as opposed to being unidirectional—I give you orders) and transitivity (the extent to which one individual's associates are associated with each other).[68] Social network analysis was developed as a research tool for understanding human relationships and organizations.[69] It is also being developed as a tool to diagnose communications bottlenecks and other

---

[64] Danezis, *supra* note 5, § 2.

[65] *See* Greenblatt et al., *supra* note 15, at 333.

[66] For a discussion of social network metrics, see, e.g., Barabási, *supra* note 7, at 25–40; Watts, *supra* note 7, at 39–40; Martin G. Everett & Stephen P. Borgatti, *Extending Centrality*, *in* Models and Methods in Social Network Analysis, *supra* note 7, at 57, 58–68; Strandburg et al., *supra* note 7, at 1301–02.

[67] Strandburg et al., *supra* note 7, at 1302, 1305.

[68] *Id.* at 1301, 1306–07.

[69] *See* Watts, *supra* note 7, at 13.

problems in existing business organizations and, alternatively, to identify key players in known terrorist or criminal networks.[70]

There are several ways in which one might consider employing social network metrics in a law enforcement or antiterrorism context. For example, associational patterns within a known network might be used to identify those playing key roles in hopes of deploying strategies to destabilize or undermine the networks.[71] Because this kind of analysis focuses on known individuals, it is not very likely to chill expressive activity unless it is abused to study groups identified by their political or other legitimate activities. This Article focuses on two other applications of network analysis—targeted "link analysis" and "pattern analysis"—that are employed to *identify* associations that are not already known.[72] Targeted "link analysis" focused on a particular individual would be used to determine the associative groups to which that individual belongs.[73] Much more ambitiously, network "models" of malevolent associations might be developed and data mining techniques used for "pattern analysis" in the hope of identifying terrorist or other criminal or socially troublesome networks.[74]

All of these approaches are in their infancy and pose potential civil liberties issues, but targeted link analysis and pattern analysis are both less well-developed and far more troubling than the use of social network metrics to analyze known networks. For one thing, the properties of social networks are such that most individuals in the United States are connected by a surprisingly small number of associative links (the so-called "small world" property).[75] Targeted link analysis and pattern analysis, which rely on analyzing networks of communications patterns, thus have the potential to sweep in a very large number of individuals and their associations in short order. Pattern analysis, especially in its most ambitious guises, would require access to very large databases of mostly innocent traffic data. It would subject the persons associated with that data (nearly everyone in the case of the allegedly government-acquired AT&T database, for example) to the

---

[70] *See, e.g.*, Carley et al., *supra* note 7, at 82; Rob Cross et al., *Six Myths About Informal Networks—And How to Overcome Them*, *in* Creating Value with Knowledge: Insights from the IBM Institute for Business Value 47, 57–58 (Eric L. Lesser & Laurence Prusack eds., 2004); Greenblatt et al., *supra* note 15, at 343–47; Klerks, *supra* note 7, at 54–58.

[71] Klerks, *supra* note 7, at 58–63.

[72] *See* K.A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 Colum. Sci. & Tech. L. Rev. 2, 34 (2003).

[73] *Id.*

[74] *See id.*

[75] *See* Barabási, *supra* note 7, at 41–54; Watts, *supra* note 7, at 37–42.

risk of adverse government action as a result of mistake or more insidious abuse by government actors.[76]

Roughly, applications of social network analysis to relational surveillance can be placed into the below hierarchy of increasing intrusiveness and decreasing accuracy.

1. Analysis of Known Social Networks

One application of social network analysis is to analyze the structure of relationships between a group of individuals already suspected of criminal or terrorist activity so as to identify key individuals and roles played by various other individuals.[77] Though it employs more sophisticated algorithms, such analysis of relationships between already identified individuals is simply a twenty-first century version of tried and true investigative techniques such as mapping out links between people on a chalkboard. Of course, even this kind of analysis is somewhat intrusive, as is any surveillance of a group's activities. Moreover, though there is a relatively robust literature of studies of existing well-defined networks upon which such an analysis can be based, that research suggests that it is often not possible to identify those playing key roles using relational data alone.[78] Although network analysis of groups of known individuals might even reduce intrusive surveillance by focusing wiretapping and other intrusive real-time surveillance on key individuals, relying on relational data could also result in a mistaken focus on minor players in a malevolent association (and in underestimating the role of important players).

Whatever the accuracy and eventual usefulness of social network analysis as applied to groups of known individuals, it seems unlikely to have much of a chilling effect on legitimate association as long as the group to be studied is identified in a legitimate fashion. Social network analysis can be applied to any group. Though there is little to worry about if law enforcement officials use it to identify the roles played by individuals known to belong to a criminal gang or terrorist organization, like any surveillance technique the technology for analyzing known networks can be abused. Social network analysis could be used by government officials in a "rogue" fashion for personal or political

---

[76] *See Hepting*, 439 F. Supp. 2d at 978.

[77] *See* KOLDA ET AL., *supra* note 7, at 15; SEIFERT, *supra* note 7, at 3; Klerks, *supra* note 7, at 58–63; Keefe, *supra* note 7; Memon & Larsen, *supra* note 7, § 2; Macskassy & Provost, *supra* note 7, § 1.

[78] *See* SEIFERT, *supra* note 7, at 3.

purposes such as identifying key targets for harassment. Such misuse of government surveillance apparatus is certainly not far-fetched—reported instances range from the infamous COINTELPRO operation of the 1960s and '70s[79] to more recent instances of police using government databases to "stalk women, threaten motorists and settle scores."[80] In such a scenario, the use of social network analysis is only one component of an enduring and significant concern about surveillance of political or religious expressive associations.[81] Where network analysis really raises the stakes, though, is when it is used to *identify* "suspicious" individuals through their associations. Use of network analysis to identify associated individuals is the focus of this Article.

2. Targeted Link Analysis to Uncover and Categorize Associations

A targeted link analysis begins with a particular "suspicious" individual and analyzes the web of relationships in which that individual is embedded.[82] In the applications at issue in this Article, the relationships would be identified using communications traffic data, though other data could be used to supplement it. Individuals would be treated as "nodes" in a communications network.[83] Links would be added between nodes in the network when there are telephone calls or email messages between them.[84] Depending on the analysis algorithm, the link might be weighted more heavily the more often the two individuals have communicated or if there are other known connections between them.[85] Importantly, a network of communications can be mapped out like this even if law enforcement officials have no access to the *contents* of the communications.

One purpose of targeted "link analysis" would be to identify and separate out the associational groups to which the target individual

---

[79] Fisher, *supra* note 11, at 631.

[80] *See* Fisher, *supra* note 11, at 623–34 (providing a historical overview of overreaching political surveillance); M. L. Elrick, *Cops Tap Database to Harass, Intimidate: Misuse Among Police Frequent, Say Some, but Punishments Rare*, Detroit Free Press, July 31, 2001, at A1.

[81] *See generally* Fisher, *supra* note 11 (analyzing politically motivated surveillance).

[82] Taipale, *supra* note 72, at 75; van Meter, *supra* note 7, at 70–72; Kathleen M. Carley, Dynamic Network Analysis for Counter-Terrorism 15–16, http://www.spcomm.uiuc.edu/TECLAB/aon/CarleyPaper.pdf (last visited Mar. 4, 2008).

[83] Taipale, *supra* note 72, at 75; van Meter, *supra* note 7, at 70–72; Carley, *supra* note 82, at 15–16.

[84] Taipale, *supra* note 72, at 75; van Meter, *supra* note 7, at 70–72; Carley, *supra* note 82, at 15–16.

[85] Taipale, *supra* note 72, at 75; van Meter, *supra* note 7, at 70–72; Carley, *supra* note 82, at 15–16.

belongs by using the patterns of connections centered on the target individual.[86] For example, suppose the target individual communicates with her family, her religious community, a political group, and a terrorist organization. Because the target individual communicates with all of these groups, her own traffic data alone is probably not sufficient to distinguish them. To separate these groups, the network analyst will want to use not only the target individual's traffic records, but the communications traffic records of those she has called or emailed, those they have called and emailed, and so forth. Network analysis algorithms use the communications patterns between these second and third order individuals to determine how the target individual's contacts are related to one another: it is anticipated that the family members will tend to call the target individual and each other, but not the political group members, and so forth. This is the kind of investigation that is suggested by a recent report that the Federal Bureau of Investigation (the "FBI") had sought call records from Verizon "not just on original targets and the people they had called, but on everyone that those people in turn had called."[87]

Link analysis is more intrusive than studying a previously identified network because it may cast suspicion on individuals, who previously have not been targeted, solely on the basis of their communications with the targeted individual—or even solely based on communications with those who communicate with the targeted individual. Indeed, that is its purpose. Because even target individuals who are rightly suspected of criminal or terrorist activity are generally part of a variety of social groups, targeted link analysis is likely to expose and analyze many entirely legitimate and innocent associations. Of course, if the target is mistakenly or maliciously selected, only innocent associations will be revealed.

Like "transactional surveillance" involving data aggregation more generally, link analysis threatens individual autonomy and has potential chilling effects because it may expose associations with groups that may be socially disfavored or simply discordant with an individual's public "persona."[88] Just as "dataveillance" can chill an individual's experimen-

---

[86] Carley, *supra* note 82, at 15–16.

[87] Eric Lichtblau, *Phone Utilities Won't Give Details About Eavesdropping*, N.Y. TIMES, Oct. 16, 2007, at A21.

[88] *See, e.g.*, SOLOVE, *supra* note 6, at 44–47; Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1425 (2000). *See generally* Slobogin, *Transaction Surveillance*, *supra* note 6 (discussing the scope and regulation of transactional surveillance).

tation with particular ideas or pastimes,[89] relational surveillance can chill tentative associations and experimentation with various group identities. Accuracy is also an issue with link analysis.[90] The data itself may give an inaccurate picture of the relationships (it is not always clear who is actually using a particular phone number or Internet account, for example) and the network analysis algorithm will not always partition associations correctly.[91] If a targeted individual belongs to a terrorist organization, a political organization, and a religious organization, for example, and those organizations have overlapping memberships, the network analysis might mistakenly categorize a member of the legitimate political organization as a member of the terrorist organization.

Though these caveats suggest that targeted network analysis should be regulated to protect both privacy and freedom of association, it must be recognized that traditional policing involves a form of targeted link analysis. Seeking to uncover possible co-offenders by interrogating the "known associates" of a suspect is a tried-and-true law enforcement technique which certainly predates, and survives, the Bill of Rights. The type of targeted link analysis potentially enabled by digital communication records and modern data analysis is not merely the equivalent of this time-tested law enforcement strategy, however. Three things have changed. First, the ubiquity of digital communications technology and the availability of inexpensive data storage means that a more and more complete record of communications traffic is available or might be made available if data retention were mandated. Second, the science of network analysis is developing to permit more sophisticated analysis of networks of relationships. Third, increasing computational power makes it possible and relatively inexpensive to analyze increasingly large networks. The ease of data acquisition and the possibility of computerized analysis dramatically broaden the net of relationships that might be routinely and inexpensively investigated. In the past, as a result of resource limitations and sensible investigative techniques, investigators would likely follow up chains of links between individuals only after learning something at each stage that warranted the expense and effort involved in following up. So, for example, upon obtaining a list of

---

[89] Roger Clarke, *Information Technology and Dataveillance*, 31 COMM. ACM 498, 498, 499 (1988) (coining the term "dataveillance").

[90] Slobogin, *Government Data Mining*, *supra* note 6, at 7.

[91] *See, e.g.*, M. Girvan & M.E.J. Newman, *Community Structure in Social and Biological Networks*, 99 PROC. NAT'L ACAD. SCI. 7821, 7823–26 (2002) (providing a discussion of a clustering algorithm and its accuracy and computational expense).

phone numbers dialed by a criminal suspect, law enforcement officers would identify these individuals and follow up only on those who seemed likely to be involved in criminal activity. The effect of such a stage-by-stage approach is to limit the range of innocent associations exposed to government scrutiny, both by limiting intrusion into the relationships of those whose connections to the target individual are not suspicious, and by providing information that might exonerate an erroneously targeted individual at an early stage.

Current digital communications make it easier to take a dragnet approach to analyzing a large network of communications. Recent complaints by FBI field offices of being swamped by meaningless "leads" for counterterrorism investigation suggest that some such dragnet approach has been taken by the government in recent years.[92] In its unfettered form, targeted link analysis can involve obtaining and mapping out the complete web of relationships surrounding a particular individual. Such a map might include the communication patterns of associates of the target, their associates, and so forth, and would be likely to uncover a much broader swath of legitimate expressive association than traditional police work. Indeed, in light of the "small world" property of many networks, extending the network out a few links from the center might draw in entire communities.[93]

3. Pattern-Based Social Network Analysis

Unlike targeted link analysis, pattern-based analysis has no direct analog in traditional law enforcement techniques, though it bears some similarity to the use of profiling to identify suspicious individuals. The goal of pattern-based analysis is to identify suspicious groups from their communications patterns without having an independent basis to suspect any target individual.[94] Pattern-based analysis, like similar data mining techniques used in other contexts, seeks to identify patterns and clusters within a large dataset using information implicit in the data, along with historical "examples" of the patterns sought.[95] For example, one of the most well known uses of data mining is to identify credit card fraud.[96] Data mining techniques find pat-

---

[92] *See, e.g.*, Lowell Bergman et al., *Domestic Surveillance: The Program; Spy Agency Data After Sept. 11 Led FBI to Dead Ends*, N.Y. TIMES, Jan. 17, 2006, at A1.

[93] *See* BARABÁSI, *supra* note 7, at 41–54 (discussing the "small world" problem); WATTS, *supra* note 7, at 37–42 (same).

[94] Taipale, *supra* note 72, at 33.

[95] *Id.* at 22–24.

[96] *See* Swire, *supra* note 2, at 964.

terns of transactions (such as a small purchase at a gas station followed by an unusually expensive purchase or a rapid succession of unusually expensive purchases) commonly associated with fraud.[97]

Pattern-based analysis could in principle be used to search through an entire database of communications records, such as the AT&T database of call traffic data allegedly made available to the Bush administration.[98] Though it is not known exactly what algorithms for pattern-based analysis have been developed by government computer scientists, what is known from basic research into network analysis suggests that computational and algorithmic limitations make this kind of super-surveillance more of a dream (or nightmare) than a reality in the near term. A more likely application of pattern-based analysis might be to a class of individuals—such as a religious, ethnic, or political group or a geographic community—believed particularly likely to include a criminal or terrorist subgroup.

Pattern-based analysis raises many very troubling issues relating both to the broad swath of communications that must be involved by the very nature of the analysis and to the likelihood of errors. Government attempts to identify criminal or terrorist networks through pattern-based data mining are likely to be far less effective and have far more negative consequences than typical commercial data mining schemes such as those used to fight credit card fraud or to target advertising.[99]

A first stage of pattern-based analysis would seek to identify relatively strongly associated groups in a traffic data network using a clustering-type algorithm.[100] A second stage would look for "signatures" of a particular type of group (such as a criminal or terrorist network) either by analyzing previous examples or using some kind of theoretical model.[101] Once such signatures are identified, existing networks can be probed for "matching" associations.[102] Pattern-based network analysis can be highly intrusive since it seeks to find a few malevolent associations in a haystack of much more numerous legitimate relationships. Clustering algorithms will reveal vast numbers of legitimate associational groups along with those malevolent groups. Some of these will be

---

[97] *See id.*; Keefe, *supra* note 7.

[98] *See Hepting*, 439 F. Supp. 2d at 978–80.

[99] *Id.*; Slobogin, *Government Data Mining*, *supra* note 6, at 7; Swire, *supra* note 2, at 964; Keefe, *supra* note 7; *cf.* Taipale, *supra* note 72, at 72.

[100] Taipale, *supra* note 72, at 28–29, 34, 60–61.

[101] *Id.* at 34, 46, 48, 60–63.

[102] *Id.*

associations that have, for perfectly legal reasons, decided not to identify themselves by membership lists and public "platforms" or agendas or have not gelled into formal associations. Network analysis can thus provide the equivalent of association membership lists without a direct request or even notice to members of a group that the government has taken an interest in their activities.[103]

Exposing legitimate, yet unpopular or fringe, associations poses a variety of threats to freedom of association. Associations, no less than individuals, can be targeted by government officials for nefarious reasons once they are identified. Further, as discussed above, the potential that an individual's association with nonmainstream groups or explorations of nonmainstream ideas will be exposed to the government threatens to chill association even more than the exposure of a membership list of a traditional group. Commercial data mining activities for targeting advertising or combating fraud mostly focus on collecting information about individuals rather than associations, though this is probably changing with the popularity of social networking sites, such as Facebook and MySpace. There is clearly a difference, however, when the miner is the government and the traffic records come from the providers of basic communication facilities such as telephone and email. One can opt out of social networking sites entirely or limit the associations reflected in them. One should not have to opt out of the telephone system or, in today's world, out of Internet communication in order to pursue legitimate, but nonmainstream, expressive associations.

Pattern-based analysis is also likely to be riddled with errors. The accuracy of pattern-based analysis of a network depends on the accuracy of the underlying data, the accuracy of the clustering algorithm used to map out associational groups within a network of traffic data, and the accuracy of the pattern or model used to identify suspicious or malevolent groups.[104] Telephone and internet traffic data are accurate only to the extent that a particular number or account can be attached to a particular individual. More importantly, clustering algorithms (rules for identifying groups) applied to large networks are not particularly accurate.[105] They are, in fact, least likely to be accurate in identifying loosely coupled organizations, such as many criminal and terrorist organizations that seek to minimize the density of traceable communi-

---

[103] *See infra* notes 227–275 and accompanying text (discussing cases regarding association membership lists).

[104] *See* Slobogin, *Government Data Mining*, *supra* note 6, at 7.

[105] *See, e.g.*, Girvan & Newman, *supra* note 91, at 7823–26.

cations between members.[106] The development of network clustering algorithms is an area of current research and algorithms are certain to improve.[107] To some extent, however, these difficulties are inherent in the structure of social networks. As mentioned above, social networks tend to be very closely connected (perhaps they are even "small world networks").[108] This makes the network of associations difficult to disentangle as a computational matter. Mistaken identifications are inevitable.

Once associative groups are identified, there remains the question of distinguishing malevolent associations from legitimate associations. Here the problems are quite deep. Terrorist events, for example, are thankfully rare. This means, however, that coming up with accurate "patterns" for terrorist networks is a difficult, if not impossible task.[109] This situation can be contrasted with the situation involving data mining to detect credit card fraud. Credit card companies have a lot of experience with fraud and much of it follows similar patterns, so the models of "fraudulent purchasing behavior" that are used in the analysis can be reasonably accurate.[110]

Even if a set of model network properties could be derived that would fit most possible terrorist networks (thus minimizing the problem of false negatives), there is likely to be a huge problem with false positives. There is, at least at this point, little reason to assume that terrorist networks will have different relational structures than many other legitimate networks.[111] Moreover, to the extent that the network structure of terrorist networks reflects their most obvious difference from typical social networks—their covert nature—it may very well be similar to the structures of the most sensitive of political networks, those involving unpopular ideas or disfavored groups.

---

[106] Greenblatt et al., *supra* note 15, at 344 ("Covert organizations generally do not have many paths of communications flow between individuals. Redundant paths lead to increased risk of exposure or capture."); Valdis E. Krebs, *Uncloaking Terrorist Networks*, 7 First Monday, Apr. 2002, http://firstmonday.org/issues/issue7_4/krebs/index.html (mapping the network of relations between the September 11th hijackers and discussing the difficulty in identifying terrorist networks before the fact).

[107] *See, e.g.*, Filippo Radicchi et al., *Defining and Identifying Communities in Networks*, 101 Proc. Nat'l Acad. Sci. 2658, 2658 (2004).

[108] *See* Barabási, *supra* note 7, at 41–54; Watts, *supra* note 7, at 37–42.

[109] *See, e.g.* Keefe, *supra* note 7; Krebs, *supra* note 106; *see also* Jonathan D. Farley, Editorial, *The N.S.A.'s Math Problem*, N.Y. Times, May 16, 2006, at A25.

[110] *See* Swire, *supra* note 2, at 964–65; Keefe, *supra* note 7.

[111] *See* Greenblatt et al., *supra* note 15, at 331–33, 344 (discussing the possibility of detecting terrorist networks on the basis of their "covert" nature); Keefe, *supra* note 7.

Pattern-based mining of traffic data is thus likely to be plagued with both false positives and false negatives to an unacceptable degree. Despite these problems, however, law enforcement entities may be motivated to employ these methods even when they are not "ready for prime time." Here again, the contrast with data mining in the credit card fraud context is instructive. Credit card companies generally pay the cost of false negatives (failure to identify fraud) because most reimburse the victims of credit card fraud for the cost of fraudulent purchases and thereby internalize those costs. False positives, on the other hand, are generally resolved with little difficulty simply by contacting the card holder and verifying the suspect transactions.[112] The ramifications of a false positive are minimal in the credit card fraud context.[113] The ramifications of errors are even more minimal in the advertising context, where the worst that can happen is that the "wrong" individual receives or does not receive an advertisement.

Like credit card companies, law enforcement entities—or at least those higher-ranking individuals who would make the decisions to employ pattern-based analysis—are likely to internalize the expected costs of false negatives (failure to identify a malevolent network) and to be much less sensitive to the costs of false positives. There are certainly social costs involved in following up useless leads[114]—indeed the monetary costs alone could be substantial—but although law enforcement officers on the front lines may complain about them, they may not be highly salient to those making the decisions about whether to pursue high tech law enforcement strategies (who are probably highly sensitive to political pressures often reflecting the glamour of "security theater" more than the mundane day-to-day pursuit of traditional investigative procedures).[115]

Unlike in the case of credit card fraud, however, the costs of false positives to those brought under suspicion by an inaccurate network analysis would be large. Unfortunately, those costs might not be felt by the government officials who decide whether to use the methods. Although public opinion might react to the harm caused by false positives

---

[112] Swire, *supra* note 2, at 964.

[113] *Id.*

[114] *See* Bergman et al., *supra* note 92.

[115] *See, e.g.* Bruce Schneier, Beyond Fear: Thinking Sensibly About Security in an Uncertain World 38–40 (2003) (discussing the idea that the concept of security is partially a state of mind, and thus, some countermeasures are intended to provide merely the feeling of security rather than actual security; or in other words, "they are nothing more than security theater").

if the methodology is sufficiently flawed that it ensnares large enough numbers of innocents, it is quite possible—probably likely—that false positives will be concentrated on socially disfavored groups. Thus, the hidden costs of unnecessary and intrusive investigations and the chilling of legitimate association, though potentially great and of great importance to a democratic society, might not cause sufficient discomfort to the majority of citizens to result in a political rejection of flawed network analysis methods. False positives, in the form either of inaccurate assignment of individuals to malevolent groups or of inaccurate characterization of groups as illegitimate, thus have a high potential to chill association, especially association of the emergent and tentative sort that is of increasing importance in the current technological milieu.

Network analysis also promotes a pernicious tendency toward the accumulation of increasing amounts of data about individuals and their interactions. When network analysis is ineffective there will always be a tendency for law enforcement to argue (with some basis) that more data would improve the accuracy of the analysis. Unrealistic expectations about the extent to which additional data can improve the analysis are likely to lead to the amassing of increasingly pervasive databases of personal and relational information in the hope of finding a foolproof method of identifying malevolent associations. The tendency to take steps in the name of security without much regard for whether they are worth the social and economic costs is already evident in other arenas.[116]

III. The Failure of Existing Legal Paradigms to Protect Association in a Networked Society

Relational surveillance is particularly threatening to democracy because of the critical role that collective behavior plays in effectuating political and social change. Complete relational surveillance could make it virtually impossible (or at least impractical) for citizens to associate anonymously to pursue a particular social goal and could deter even the exploration of controversial ideas and positions. The U.S. Supreme Court has recognized the importance to democracy of citizens' ability to associate away from the prying eyes of government by striking down as unconstitutional various government requirements that political groups turn over their membership lists.[117] Subpoenas for association membership lists are also frequently quashed on First Amendment

---

[116] *See id.*

[117] *See infra* notes 227–275 and accompanying text.

grounds.[118] This existing protection from disclosure of membership lists, however, is no longer sufficient to uphold the right to associational freedom. These are exciting times precisely because of the opportunities for new ways of associating to pursue collective goals that are provided by the Internet and other communication technologies. Relational surveillance threatens to undermine the potential of these new ways of associating by providing the government with means to obtain information about group membership, which evade the legal strictures on direct inquiry to a traditional association. Freedom of association doctrine has yet to grapple with the ways in which technology has changed associational patterns. Meanwhile, surveillance law has failed to develop a jurisprudence of freedom of association because surveillance questions have been analyzed solely from within a privacy paradigm.[119] Because surveillance law has focused on individual privacy and neglected First Amendment concerns, it provides its lowest protection to noncontent, traffic data that is in third party hands, leaving a major gap in current protection of the right to freedom of association.[120]

A. *The Fourth Amendment and Relational Surveillance*

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[121] Under Supreme Court case law, the inquiry as to whether there has been an "unreasonable search" begins with a determination as to whether a "search" has occurred.[122] Rather than relying on common usage of the word "search," the law holds that there has been no search unless the government has intruded on an "expectation of privacy," which is both subjectively present and objectively reasonable.[123] Unless there has been a search in this sense, the Fourth Amendment has no application.[124] Once there has been a search, the Fourth Amendment, by default, requires a warrant based on probable cause.[125] The case law, however, provides numerous exceptions to the warrant requirement based on factors such as exigency,

---

[118] *See infra* notes 227–275 and accompanying text.
[119] *See infra* notes 121–207 and accompanying text.
[120] *See infra* notes 121–207 and accompanying text.
[121] U.S. CONST. amend. IV.
[122] *See* Katz v. United States, 389 U.S. 347, 353 (1967).
[123] *Id.* at 360–61 (Harlan, J., concurring).
[124] *See* Slobogin, *Government Data Mining*, *supra* note 6, at 11.
[125] U.S. CONST. amend. IV.

administrative necessity, "special needs," and so forth, most of which are beyond the scope of this Article.[126]

The Fourth Amendment as applied thus far, and even as supplemented by statutory regulation, provides little protection against relational surveillance because the Supreme Court generally has not found a reasonable expectation of privacy either in information that has been conveyed to a third party or in communication traffic data.[127] Thus, it will be difficult to convince a court that relational surveillance using traffic data involves a "search" at all given that traffic data almost by definition is obtained from communications intermediaries. Even if such relational surveillance were deemed a search, an argument could be made that broad-based network analysis is permissible under the Fourth Amendment's "special needs" doctrine.[128]

A complex statutory regime supplements the Fourth Amendment's protections against government surveillance, providing somewhat greater protection in some cases.[129] That regime, however, gives its lowest protection to noncontent traffic data and also distinguishes between real-time interception and the analysis of stored records.[130] Relational surveillance thus relies almost exclusively on types of information to which the current surveillance law regime affords the lowest levels of protection.

1. The Limited Protection Available to Information "Conveyed" to a Third Party

For regulating relational surveillance, the most troublesome aspect of Fourth Amendment doctrine as currently conceived is that it provides virtually no protection to information that has been "conveyed to a third party."[131] The understanding is that, by conveying in-

---

[126] *See* Christopher Slobogin, *Let's Not Bury* Terry*: A Call for Rejuvenation of the Proportionality Principle*, 72 St. John's L. Rev. 1053, 1062–66 (1998) [hereinafter Slobogin, *Let's Not Bury* Terry] (discussing the "danger" exception to the Fourth Amendment warrant requirement); Slobogin, *Transaction Surveillance*, *supra* note 6, at 150 nn.32–34 (citing cases regarding "stop and frisk" and "special needs" exceptions to the general warrant requirement); Steinbock, *supra* note 6, at 39–41 (discussing administrative search exceptions to the warrant requirement).

[127] *See infra* notes 131–153, 176–179 and accompanying text.

[128] *See infra* notes 161–170 and accompanying text.

[129] *See infra* notes 171–207 and accompanying text.

[130] *See infra* notes 171–207 and accompanying text.

[131] *See* Bellia, *supra* note 6, at 1402; Henderson, *Learning from All Fifty States*, *supra* note 6, at 373; Slobogin, *Transaction Surveillance*, *supra* note 6, at 149–66; Swire, Katz *is Dead*, *supra* note 6, at 910–12; Zittrain, *supra* note 6, at 83–84.

formation to a third party, an individual "assumes the risk" that the third party might disclose that information to others.[132] In its opinions, the Supreme Court has taken a very broad view of the circumstances under which information has been "conveyed" to a third party and for the most part has not been responsive to arguments based on expectations of confidentiality.[133]

In 1976, in the seminal case of *United States v. Miller*, for example, the Court determined that an individual had no Fourth Amendment interest in his bank records, which were deemed "business records of the banks."[134] The Court reasoned that the information held by the bank was regularly exposed to bank employees in the ordinary course of business and as a result, the depositor "takes the risk" that an employee might choose to convey that information to the government.[135] The Court was unswayed by arguments that banks have contractual and fiduciary obligations of confidentiality with regard to the records.[136] Particularly troubling was the Court's refusal to condition its analysis on the fact that the government *required* banks to maintain the records in question to comply with the Bank Secrecy Act.[137]

A few years later in 1979, in *Smith v. Maryland*, the Court considered whether installation of a "pen register" to record the telephone numbers dialed from a suspect's home was a "search" subject to Fourth Amendment protection.[138] Again the Court found no "reasonable expectation of privacy" and hence no Fourth Amendment protection.[139] The Court based its holding on the fact that "[t]elephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes."[140] Stating that it "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," the Court held that by dialing the phone number, the petitioner "voluntarily conveyed numerical information to the

---

[132] Smith v. Maryland, 442 U.S. 735, 744 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

[133] *See Smith*, 442 U.S. at 743–44; *Miller*, 425 U.S. at 440–43.

[134] 425 U.S. at 440, 442–45.

[135] *Id.* at 443.

[136] *Id.*

[137] *See id.* at 441.

[138] 442 U.S. at 736.

[139] *Id.* at 742.

[140] *Id.* at 743–44.

telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."[141] The Court rejected the argument that, because of automation, no human being at the phone company is actually exposed to the phone number when it is dialed, stating that "[w]e are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate."[142]

Similarly in 1984, in *Securities & Exchange Commission v. Jerry T. O'Brien, Inc.*, the Court summarized its view that "[w]hen a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities."[143]

A potential crack in the third party doctrine has appeared in the context of state hospital diagnostic tests. In 2001, in *Ferguson v. City of Charleston*, the Court held that "[t]he reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."[144] It is unclear whether this finding of a reasonable expectation of privacy in the context of a confidential doctor-patient relationship has any application outside of the medical context, where privacy interests are deemed to be especially strong.[145]

The doctrine that information conveyed to a third party loses any Fourth Amendment protection has come under increasing criticism in light of the growing extent to which private information is necessarily and routinely handled by (and recorded by) data intermediaries in the age of the Internet and in light of the increasing digitalization of voice communications. Indeed, in 1967, in *Katz v. United States*, the seminal case extending Fourth Amendment protection beyond the home and the source of the "reasonable expectation of privacy" test, the Court held that the Fourth Amendment precludes government wiretapping without a warrant.[146] Yet, telephone conversations are

---

[141] *Id.* at 744.

[142] *Id.* at 744–45.

[143] 467 U.S. 735, 743 (1984).

[144] 532 U.S. 67, 78 (2001).

[145] *See* Whalen v. Roe, 429 U.S. 589, 603–04 (1977) (holding that the patient identification requirement of a state law mandating the filing of an official form with the State Health Department when certain drugs were prescribed did not constitute an invasion of any right or liberty protected by the Fourth Amendment).

[146] 389 U.S. at 353, 357–58.

certainly conveyed to the person on the other end of the line. Moreover, they travel over telephone company wires and are handled by the phone company en route.

Outside of the communications context, moreover, the Fourth Amendment has been held to apply to physical property even when it has been entrusted to third parties for storage and transport.[147] Thus, courts have recognized a reasonable expectation of privacy in letters entrusted to the postal service, rented rooms, storage units, and sealed containers.[148] In the ordinary course of business the postal carriers, landlords, and so forth have no reason or contractual right to meddle with the contents of the relevant letters, apartments, or containers.[149]

These precedents suggest two plausible limitations on the third party doctrine. First, if *Katz* itself is to remain good law, the third party doctrine should apply only when the government obtains the information from the third party to whom it was conveyed. Thus, a participant in a telephone conversation may be subpoenaed to testify as to what was said even though the conversation could not be wiretapped without a warrant. Second, the third party doctrine should apply at most when the conveyance to a third party is for that third party's use in the ordinary course of business. When a third party merely stores or carries property on behalf of another, the owner of the property may retain a Fourth Amendment expectation of privacy if the third party has no business reason to look into the contents. Arguably, then, the third party doctrine should be limited so that the owners of computer files and email archives maintained by ISPs and other intermediaries retain Fourth Amendment interests in their contents. The Su-

---

[147] *See* United States v. Jacobsen, 466 U.S. 109, 114 (1984); Stoner v. California, 376 U.S. 483, 489–90 (1964); Chapman v. United States, 365 U.S. 610, 616–18 (1961); United States v. Johns, 851 F.2d 1131, 1133–35 (9th Cir. 1988).

[148] *See Jacobsen*, 466 U.S. at 114 (noting that, with regard to letters entrusted to the U.S. Postal Service, "[l]etters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable"); *Stoner*, 376 U.S. at 489–90 (holding that search of hotel room without warrant violated Fourth Amendment, despite the fact that one who engages a hotel room gives implied permission to hotel personnel to enter to perform their duties); *Chapman*, 365 U.S. at 616–18 (holding that search of house occupied by tenant violated Fourth Amendment, despite fact that landlord had authority to enter house for some purposes); *Johns*, 851 F.2d at 1133–35 (implicitly recognizing reasonable expectation of privacy in rented storage unit).

[149] This view of this case law is consistent with cases in which there was no reasonable expectation of privacy because, for example, rent had not been paid or property had seemingly been abandoned. *See, e.g.*, United States v. Wilson, 472 F.2d 901, 903 (9th Cir. 1972). In the ordinary course of business, landlords can be expected to intrude upon the property under such circumstances. *See id.*

preme Court has yet to consider this question. An appellate court has recently agreed with this analysis, finding that the Fourth Amendment protects email stored with an ISP, but rehearing en banc has been granted in that case.[150]

One might also argue that, even if obtaining records of traffic data is not a search, applying network analysis to the data and thus disclosing previously unknown patterns of association is a search. In 2001, in *Kyllo v. United States*, the Court held that using a thermal imager to obtain images of what is going on in the interior of a home constituted a search, despite the fact that the images were based on thermal data collected in a public space outside of the house.[151] Arguably, network analysis technology, like the thermal imager in *Kyllo*, produces new information that is not in the hands of the third parties who have collected the traffic data.[152] If the associational structure can be discerned only by applying sophisticated data mining technology, perhaps there is a "reasonable expectation of privacy" in those associations.

This argument, even if successful, is of limited use. Any reasonable expectation of privacy in associations "revealed" only by network analysis could only extend to those emergent associations whose structure and membership were unknown even to members. Once information about one's membership in an organization is shared with third parties—such as the other members of the organization—the third party doctrine as currently applied would likely destroy any reasonable expectation of privacy. Moreover, *Kyllo* is premised on strong traditional rights of privacy in the home,[153] making it a thin reed on which to base an argument for Fourth Amendment protection against relational surveillance using computerized network analysis.

2. The Limited Protection Available for Noncontent Data

Whatever the eventual result regarding the contents of email and other files maintained by third parties, courts seem unlikely to find a reasonable expectation of privacy in addressing information and other traffic data per se, if for no other reason than that it is conveyed "to" the intermediary for its use in the ordinary course of business, and is thus apparently comparable to the phone numbers collected by the

---

[150] Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007), *reh'g en banc granted*, No. 06-4092, 2007 U.S. App. LEXIS 23741, at *1–2 (6th Cir. Oct. 9, 2007).

[151] 533 U.S. 27, 30, 40 (2001).

[152] *Id.* at 40.

[153] *Id.* at 31, 40.

pen register in *Smith*.[154] In reasoning that there is no Fourth Amendment protection for phone numbers dialed, the Court relied in part on the fact that pen register data does not disclose the content of conversations.[155]

More recently, courts have applied a similar analysis to Internet subscriber data and traffic information.[156] For example, in an unpublished decision in 2000, *United States v. Hambrick*, the U.S. Court of Appeals for the Fourth Circuit held that an Internet user did not have a reasonable expectation of privacy in his subscriber information.[157] The court opined that

> [w]hile under certain circumstances, a person may have an expectation of privacy in content information, a person does not have an interest in the account information given to the ISP in order to establish the e-mail account, which is noncontent information. Disclosure of this noncontent information to a third party destroys the privacy expectation that might have existed previously.[158]

Similarly, in 2008, the U.S. Court of Appeals for the Ninth Circuit, in *United States v. Forrester*, held that "e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers . . . ."[159]

The difficulty with the distinction between "content" and "noncontent" information is that it does not recognize the extent to which a network analysis of traffic data might reveal patterns of association that are, as discussed below, protected by the First Amendment and critical to democratic liberty.[160] Moreover, even though an intermediary makes use of bits and pieces of traffic data in the ordinary course of routing and delivering communications, the associations derived by network analysis algorithms would never be apparent from the ordinary business uses to which intermediaries put traffic data. It is therefore unrea-

---

[154] *See* 442 U.S. at 743–44.

[155] *Id.* at 741–43.

[156] Unites States v. Forrester, 512 F.3d 500, 509–10 (9th Cir. 2008); United States v. Hambrick, No. 99-4793, 2000 U.S. App. LEXIS 18665, at *11–12 (4th Cir. Aug. 3, 2000).

[157] 2000 U.S. App. LEXIS 18665, at *11–12.

[158] *Id.*

[159] 512 F.3d at 510.

[160] *See infra* notes 208–275 and accompanying text.

sonable to act as though the results of network analysis are disclosed to the provider in the ordinary course of business in any meaningful sense.

3. "Special Needs" Searches

Even if network analysis of traffic data to reveal associational patterns were recognized as a search, however, it is unclear how Fourth Amendment doctrine would handle a broad program of warrantless and suspicionless relational surveillance. The Supreme Court has recognized exceptions to the warrant requirement for certain administrative and regulatory searches, such as various health and safety inspection programs.[161] In addition, "special needs" may, in certain exceptional circumstances, justify a search policy designed to serve non-law enforcement ends.[162] Though a special needs search may involve law enforcement to some degree, the Court "decline[s] to approve a program whose primary purpose is ultimately indistinguishable from the general interest in crime control."[163]

The purpose of a program of relational surveillance, however, is unlikely to be "ultimately indistinguishable from the general interest in crime control."[164] Its purpose might be to avert terrorist activity, for example. Given the importance of this objective and its focus on preventing future harm rather than on solving prior crimes, the prevention of terrorism might be deemed an appropriate "special need" justifying a deviation from the warrants and individualized suspicion requirements of the Fourth Amendment despite the fact that law enforcement purposes are also involved.[165] The inclusion by various courts of DNA databases within the "special needs" exception suggests courts' willingness to stretch the definition of non-law enforcement purposes where sufficiently important government interests appear to be at stake.[166]

A "special need" search must be reasonable under a balancing test that balances the state interest against the intrusion on individual pri-

---

[161] *See, e.g.*, Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990); Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 634 (1989); New Jersey v. T.L.O., 469 U.S. 325, 333 (1985) ("[T]he Fourth Amendment applies to searches conducted by school authorities, but the special needs of the school environment require assessment of the legality of such searches against a standard less exacting than that of probable cause.").

[162] *See Ferguson*, 532 U.S. at 79–84.

[163] City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000).

[164] *See id.*

[165] *See id.* ("[T]he Fourth Amendment would almost certainly permit an appropriately tailored roadblock set up to thwart an imminent terrorist attack . . . .").

[166] *See* United States v. Hook, 471 F.3d 766, 772–73 (7th Cir. 2006).

vacy.[167] To determine whether a search qualifies as a special need, "[t]he considerations that are examined . . . include the governmental interest involved, the nature of the intrusion, the privacy expectations of the object of the search, and the manner in which the search is executed."[168] The difficulty in using this balancing test to evaluate a relational surveillance program is that the test is not designed to take account of the important First Amendment interests implicated by relational surveillance. As discussed in more detail below, the First Amendment generally requires a compelling government interest and least restrictive means test before disclosure of an association membership list may be required.[169] No expectation of privacy in the membership list is necessary to trigger First Amendment protection.[170] Perhaps the special needs balancing test could be modified to take First Amendment interests into account, but in that case direct application of the First Amendment to evaluate the relational surveillance seems less contrived. Moreover, adapting the balancing test would not solve the significant hurdle of demonstrating that there has been a Fourth Amendment search in the first place. On balance, then, Fourth Amendment doctrine is an insufficient means to regulate relational surveillance so as to ensure that it complies with the Constitution.

B. *Low Protection for Traffic Data Under Surveillance Statutes*

Congress has supplemented the Fourth Amendment's protections with statutory surveillance law.[171] This statutory law generally follows a tiered scheme in which the level of protection is keyed to the third party and content/noncontent distinctions.[172] Moreover, the statutory

---

[167] *See* Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 665–66 (1989); Camara v. Mun. Court, 387 U.S. 523, 536–37 (1967).

[168] *Hook*, 471 F.3d at 772.

[169] *See infra* notes 208–275 and accompanying text.

[170] *See infra* notes 227–275 and accompanying text.

[171] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.); Foreign Intelligence Surveillance Act, 50 U.S.C.A. §§ 1801–1871 (West 2003 & Supp. II 2007); *see also* Dierdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1559–71 (2004) (providing a detailed discussion of the history, adoption, and construction of the Electronic Communications Privacy Act). The electronic surveillance law created by the Electronic Communications Privacy Act can be broken down into three statutes: the Wiretap Act, 18 U.S.C.A. §§ 2511–2522 (West 2000 & Supp. 2007), the Pen Register statute, 18 U.S.C. §§ 3121–3127 (2000 & Supp. IV 2004), and the Stored Communications Act, 18 U.S.C.A. §§ 2701–2711 (West 2000 & Supp. 2007); Mulligan, *supra*, at 1565.

[172] *See* Mulligan, *supra* note 171, at 1565–66.

scheme introduces a further distinction between real-time interception of communications and obtaining stored records.[173] Surveillance statutes regulate government acquisition of communications information in the law enforcement and foreign intelligence contexts.[174] For the most part, a lower threshold applies to foreign intelligence surveillance, which is authorized by a special secret court under FISA.[175] Both regimes, however, provide only minimal protection to traffic data. Thus, the statutory regulatory scheme, like Fourth Amendment doctrine, provides its lowest protection when faced with government acquisition of traffic data.

1. Statutory Regulation of Real-Time Acquisition of Traffic Data

Traffic data may be obtained either by real-time tracking or by access to stored records of communications carriers.[176] Real-time interception of communications *content* is traditionally highly constrained.[177] Thus, a "superwarrant" is required under the Wiretap Act before law enforcement agents can directly intercept the content of communications.[178] A strong showing of probable cause and particularity is required to obtain a wiretap order and the orders are granted subject to severe limitations and continuing review.[179] By contrast, government officials may record traffic data in real time based on a much lower standard.[180] Real-time acquisition of traffic data for law enforcement purposes is governed by 18 U.S.C. §§ 3121–3127, also known as the "pen register" or "trap and trace" statute because of its origins as a means of regulating particular technologies for intercepting dialed telephone numbers.[181] In its current incarnation, the statute defines "pen register" and "trap and trace device" broadly to encompass any means of recording addressing or routing information for any telephone or Internet communications.[182] Thus:

---

[173] *See id.* at 1565.

[174] *See* Bellia, *supra* note 6, at 1376–77.

[175] 50 U.S.C.A. § 1803; *see* Lichtblau & Johnston, *supra* note 39.

[176] *See* Bellia, *supra* note 6, at 1381.

[177] *See, e.g.*, *Smith*, 442 U.S. at 741–42 (distinguishing protection of content of communications vs. noncontent information).

[178] *See* 18 U.S.C. § 2518 (2000); Mulligan, *supra* note 171, at 1561.

[179] *See* 18 U.S.C. § 2518.

[180] *See id.* §§ 3121–3127 (2000 & Supp. IV 2004).

[181] *See id.*; *Smith*, 442 U.S. at 736 n.1.

[182] 18 U.S.C. § 3127.

> (3) the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication . . . ;
>
> (4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication . . . .[183]

Using these definitions, the statute prohibits the use of pen registers and trap and trace devices unless an application for a court order is made by specified law enforcement officers.[184] To obtain such a court order, the officer must certify only "that the information likely to be obtained is *relevant* to an ongoing criminal investigation being conducted by that agency."[185] Upon receiving an appropriate application containing such a certification, a court *must* issue the necessary order.[186] In the context of international terrorism, an alternative approach is available. Under FISA,[187] a pen register or trap and trace order may be obtained in relation to an investigation "to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution" upon a mere certification that the information is "relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities."[188]

Thus, although government interception of communication content is for the most part permitted only under very stringent, court-supervised conditions, traffic data may be intercepted even if it is merely "relevant" to an investigation.[189]

---

[183] *Id.* § 3127(3)–(4).
[184] *Id.* §§ 3122–3123.
[185] *Id.* § 3122 (emphasis added).
[186] *Id.* § 3123.
[187] 50 U.S.C.A. § 1842 (West 2003 & Supp. 2007).
[188] *Id.* § 1842(a)(1), (c)(2).
[189] *Compare* 18 U.S.C. § 2518 (2000), *with* 50 U.S.C.A. § 1842(c)(2).

2. Statutory Regulation of Acquisition of Stored Traffic Data

The most likely means by which government would obtain traffic data for network analysis is not real-time interception, but acquisition of records maintained by a communications carrier. Such an acquisition is at issue in the lawsuit against AT&T, for example, which alleges that AT&T, in contravention of statutory prohibitions on divulging traffic data,

> has provided the government with direct access to the contents of [various call record] databases that it manages . . . by providing the government with copies of the information in the databases and/or by giving the government access to Daytona's [a sophisticated database management system] querying capabilities and/or some other technology enabling the government agents to search the databases' contents.[190]

Modern use of digital technology drastically increases the extent to which traffic data is stored. Telephone companies and ISPs are able to maintain vast databases recording communications traffic almost indefinitely. To the extent that this stored information is deemed unprotected by constitutional strictures, statutes might in principle be passed to mandate even more storage of traffic data than these providers might choose for their own business purposes. The *Miller* case suggests that there would be no Fourth Amendment barrier to mandating such data retention.[191] If data retention is mandated, even the possibility that service providers might compete in the marketplace on the basis of greater protection of privacy by not maintaining traffic data would be eliminated.

Although the *Miller* and *Smith* cases imply that the Fourth Amendment does not restrict government access to the stored traffic data used in relational surveillance, surveillance statutes do regulate the circumstances under which the government can obtain such data[192] and prohibit service providers from disclosing such information in most circumstances.[193] The threshold, however, for obtaining communications traffic data is minimal. Under 18 U.S.C. § 2703, electronic communications records may be obtained by government officials pursuant to a

---

[190] Complaint at 12, Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006) (No. C-06-0672-JCS) *available at* http://www.eff.org/files/filenode/att/att_complaint_amended.pdf.

[191] *Miller*, 425 U.S. at 441–43.

[192] 18 U.S.C.A. §§ 2703, 2709 (West 2000 & Supp. 2007); *see Smith*, 442 U.S. at 741–43; *Miller*, 425 U.S. at 440–42.

[193] 18 U.S.C.A. § 2702.

court order based on "specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought, are relevant and material to an ongoing criminal investigation."[194] Certain records may also be disclosed pursuant to an administrative, grand jury, or trial subpoena.[195]

Even less is required in the national security context, where toll billing records may be requested using a "national security letter" ("NSL"), which may be issued without judicial oversight by certain FBI officials.[196] The request requires only a written certification that the records are "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States."[197] Other records may be obtainable using the business records provision of FISA.[198] For example, 50 U.S.C. § 1861 provides that certain FBI officials may apply

> for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation . . . to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.[199]

Application for such an order must include "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation . . . to protect against international terrorism or clandestine intelligence activities . . . ."[200]

In general, then, traffic data may be obtained by the government upon a showing of mere "relevance" (sometimes augmented by "materiality") to either a law enforcement investigation or an investigation to protect against international terrorism.[201] These requirements of "rele-

---

[194] *Id.* § 2703.
[195] *Id.*
[196] *See id.* § 2709.
[197] *Id.*
[198] 50 U.S.C.A. § 1861 (West 2003 & Supp. 2007).
[199] *Id.*
[200] *Id.*
[201] 18 U.S.C.A. §§ 2703, 2709; 50 U.S.C.A. § 1861.

vance" and "materiality" provide a low hurdle to obtaining traffic data. Oversight is also minimal, because courts often are required to issue these orders as long as the proper attestations are made, and in cases where NSLs may be used no court order is required at all.[202] Recent internal audits of FBI usage of NSLs demonstrate the dangers of such an unsupervised regime, with NSLs increasingly being used to obtain personal information concerning American citizens.[203] In a review of ten percent of the NSLs issued from 2002 through 2005, moreover, more than one thousand were found to have been issued contrary to statute or regulations.[204] Persons to whom NSLs pertain often are given no notice that the records are being turned over, and third party holders of the data are in many cases prohibited from disclosing that they received such a request.[205] This statutory scheme, like the Fourth Amendment doctrine on which it builds, clearly presumes that the intrusiveness of government access to traffic data is minimal.

Relational surveillance using network analysis sits uncomfortably in this statutory scheme. How many "links" away in the network of communication must an individual be before his or her traffic data is no longer "relevant" or "material" to an investigation that begins with reason for suspicion of some central individual? Does the answer to this question depend on the algorithm that law enforcement officials intend to employ? How large a sample of the network is needed if, say, the objective of a link analysis is to understand the role that the central individual plays in his or her associational network? Even more importantly, if a pattern analysis is intended, how complete must the network be before patterns can be classified and nodes clustered in a meaningful way? Arguably, the accuracy of any large scale data analysis algorithm is improved by including more data in the analysis. The scope of relevance could extend quite far, particularly where law enforcement interpretation is unfettered by meaningful judicial oversight.

Under current statutes, the potential First Amendment implications of disclosing traffic data are barely acknowledged. FISA's limitations on investigations "conducted solely upon the basis of activities

---

[202] *See* 18 U.S.C.A. § 2709; 18 U.S.C. § 3123 (2000 & Supp. IV 2004).

[203] *See* Dan Eggen, *FBI Found to Misuse Security Letters: 2003-06 Audit Cites Probes of Citizens*, WASH. POST, Mar. 14, 2008, at A3; John Solomon, *FBI Finds It Frequently Overstepped in Collecting Data*, WASH. POST, June 14, 2007, at A1.

[204] Solomon, *supra* note 203.

[205] *See, e.g.*, Editorial, *My National Security Letter Gag Order*, WASH. POST, Mar. 23, 2007, at A17. Note, however, that a district court has ruled that the nondisclosure provision is an unconstitutional suppression of speech. Doe v. Gonzales, 500 F. Supp. 2d 379, 425 (S.D.N.Y. 2007).

protected by the first amendment to the Constitution" would apply only to the most egregious harassment.[206] Indeed, without meaningful judicial oversight, this provision is essentially toothless and unlikely to deter any law enforcement official bent on reproducing the excesses of the Hoover era.[207] As the next Section explains, the important freedom of association implications of relational surveillance demand a more searching First Amendment analysis.

C. *Relational Surveillance and the First Amendment*

Although the Fourth Amendment and associated surveillance statutes provide minimal protection against relational surveillance using traffic data, the First Amendment strongly protects freedom of association in other contexts. The Supreme Court's recent First Amendment jurisprudence provides strong protection to formal associations and recognizes the important role of freedom of association in a democratic society.[208] A separate line of cases recognizes the importance of being able to associate without government inquiry into association membership.[209] Specifically, the First Amendment shields membership lists of expressive associations from government acquisition unless a strict scrutiny hurdle is surmounted.[210] These cases, which provide limits on government's ability to inquire into association membership, must be adapted to today's new associational paradigms and new technical means to acquire information about group affiliation.

1. Free Association as an Important First Amendment Interest

Constitutional protection of freedom of association and the right of assembly is deep-rooted. The right of assembly and to petition the government is explicit in the First Amendment's text.[211] The more general right to freedom of association is implicit but longstanding and strong.[212] In 2000, in the Supreme Court's most recent case on this subject, *Boy Scouts of America v. Dale*, the Court recognized the crucial role of association in democratic life and strongly upheld the right of "ex-

---

[206] *See* 50 U.S.C.A. §§ 1842, 1861 (West 2003 & Supp. 2007).

[207] *See* Fisher, *supra* note 11, at 629–30 (discussing this history).

[208] *See* Boy Scouts of Am. v. Dale, 530 U.S. 640, 647–48 (2000); Roberts v. U.S. Jaycees, 468 U.S. 609, 622 (1984).

[209] *See infra* notes 227–275 and accompanying text.

[210] Buckley v. Valeo, 424 U.S. 1, 64 (1976); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 460–63 (1958).

[211] U.S. CONST. amend. I.

[212] *See Buckley*, 424 U.S. at 15.

pressive associations" to determine their own membership requirements and policies.[213] The Court observed that:

> "[I]mplicit in the right to engage in activities protected by the First Amendment" is "a corresponding right to associate with others in pursuit of a wide variety of political, social, economic, educational, religious, and cultural ends." This right is crucial in preventing the majority from imposing its views on groups that would rather express other, perhaps unpopular, ideas.[214]

The Court's definition of an "expressive association" deserving protection is broad: "[A]ssociations do not have to associate for the 'purpose' of disseminating a certain message in order to be entitled to the protections of the First Amendment. An association must merely engage in expressive activity that could be impaired in order to be entitled to protection."[215] In *Dale*, freedom of association trumped important state interests in addressing discrimination against gays despite the fact that the Boy Scouts' evidence that it had associated to express a position on homosexuality was quite weak.[216] Indeed, the Court was willing to "accept the Boy Scouts' assertion [that it did not want to promote homosexual conduct as a legitimate form of behavior]" and opined that it "need not inquire further to determine the nature of the Boy Scouts' expression with respect to homosexuality," considering evidence of the group's position on homosexuality only as "instructive, if only on the question of the sincerity of the professed beliefs."[217] The Court not only "give[s] deference to an association's assertions regarding the nature of its expression, [but] . . . also give[s] deference to an association's view of what would impair its expression."[218]

Once an association meets this deferential standard for asserting that its rights to expressive association would be impaired by a particular government action, the government action is allowed only if it is "adopted to serve compelling state interests, unrelated to the suppression of ideas, that cannot be achieved through means significantly less

---

[213] 530 U.S. at 647–48.

[214] *Id.* (quoting and citing *Roberts*, 468 U.S. at 622, for the proposition that "protection of the right to expressive association is 'especially important in preserving political and cultural diversity and in shielding dissident expression from suppression by the majority'").

[215] *Id.* at 655.

[216] *See id.* at 650–53, 659.

[217] *Id.* at 651.

[218] *Dale*, 530 U.S. at 653.

restrictive of associational freedoms."[219] In the *Dale* case, the Court found that New Jersey's interest in undermining discrimination against homosexuals was not a sufficiently compelling interest to justify requiring the Boy Scouts to retain an openly homosexual troop leader.[220] Whatever one thinks of the result in this particular case (and it invoked strong dissent),[221] the point for our purposes is this: expressive association, broadly defined, is afforded the highest protection under the First Amendment.[222] Government impositions on freedom of association must meet the standards of strict scrutiny.[223] Courts must defer to an association's view of what would impair its expressive activities.[224] There is no reason for freedom of association rights to be checked at the doorway to cyberspace.

It is not immediately clear how the strong protection of expressive association evident in *Dale* should be applied to less traditional organizations. Emergent associations may not have well-defined "positions" on issues, or a well-defined hierarchy, or even a well-defined membership that can determine who can speak for the group and assert the group's rights. Moreover, relational surveillance does not directly regulate the messages that groups can express but merely attempts to determine who is associated with whom. Nonetheless, relational surveillance implicates the same important First Amendment interests in protecting the "right to associate with others in pursuit of a wide variety of . . . ends" and "preventing the majority from imposing its views on groups that would rather express other, perhaps unpopular, ideas" recognized by the Court in *Dale*.[225] The fact that an organization uses email and other forms of digital communications should not be allowed to vitiate its members' associational rights, particularly where some of this communication involves core political association.

As discussed above, relational surveillance impairs expressive activities not directly through regulation, but indirectly through deterrence.[226] The burdens imposed by relational surveillance in the form

---

[219] *Id.* at 648 (citing *Roberts*, 468 U.S. at 623).

[220] *See id.* at 659–61.

[221] *Id.* at 696 (Stevens, J., dissenting) ("The only apparent explanation for the majority's holding, then, is that homosexuals are simply so different from the rest of society that their presence alone—unlike any other individual's—should be singled out for special First Amendment treatment.").

[222] *See id.* at 647–48 (majority opinion).

[223] *Dale*, 530 U.S. at 648; *Roberts*, 468 U.S. at 623.

[224] *Dale*, 530 U.S. at 653.

[225] *Id.* at 647–48.

[226] *See supra* notes 31–36 and accompanying text.

of network analysis are of at least three types: chilling of protected association by revealing its existence, structure, and membership; chilling of protected association because of the potential for network analysis to mistake legitimate association for illegitimate association; and harms to self-determination and chilling of exploratory associations because of the potential for network analysis to treat individuals as "members" of a group with which they did not want to associate themselves. These are the types of harms traditionally associated with a line of freedom of association cases dealing with government requests for association membership lists.

2. First Amendment Protection of Membership Lists

In a series of cases beginning in the 1950s, the Supreme Court recognized that a government-mandated disclosure of group membership could be an unconstitutional infringement on the right of association.[227] In 1958, in *NAACP v. Alabama ex rel. Patterson*, the Court first determined that the NAACP had standing to assert the associational rights of its members because "to require that [the right of association] be claimed by the members themselves would result in nullification of the right at the very moment of its assertion."[228] The Court went on to note the importance of freedom of association:

> Effective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association, as this Court has more than once recognized by remarking upon the close nexus between the freedoms of speech and assembly. It is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the "liberty" assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech. Of course, it is immaterial whether the beliefs sought to be advanced by association pertain to political, economic, religious or cultural matters, and *state action which may have the effect of curtailing the freedom to associate is subject to the closest scrutiny.*[229]

---

[227] *See* Brown v. Socialist Workers '74 Campaign Comm. (Ohio), 459 U.S. 87, 91 (1982); *Buckley*, 424 U.S. at 64; *NAACP v. Alabama*, 357 U.S. at 460–61.

[228] 357 U.S. at 459.

[229] *Id.* at 460–61 (emphasis added) (citations omitted).

The Court also noted the potential for state actions to have the unintended effect of curtailing freedom of association: "In the domain of these indispensable liberties, whether of speech, press, or association, the decisions of this Court recognize that abridgement of such rights, even though unintended, may inevitably follow from varied forms of governmental action."[230] It also "recognized the vital relationship between freedom to associate and privacy in one's associations."[231] Indeed, the Court noted that "[i]nviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."[232] Finding the state's interest in requiring production of a membership list insufficient to justify the potential intrusion on protected association, the Court struck down an Alabama statute requiring disclosure.[233]

The right to freedom of association is not absolute, of course, and in later cases courts have addressed the limitations of the right to avoid disclosing the identities of members of a group.[234] The most widely cited case in this regard, the Supreme Court's 1972 decision in *Laird v. Tatum*, deals not with membership lists per se, but with a program of Army surveillance of political activity that involved attending demonstrations and group meetings.[235] The surveilled activity was undeniably protected by the First Amendment, but the Court nonetheless denied relief.[236] The question presented by the case was one of standing:

> [W]hether the jurisdiction of a federal court may be invoked by a complainant who alleges that the exercise of his First Amendment rights is being chilled by the mere existence, without more, of a governmental investigative and data-gathering activity that is alleged to be broader in scope than is reasonably necessary for the accomplishment of a valid governmental purpose.[237]

The Court noted that it was "significant that the principal sources of information [gathered by the surveillance program] were the news

---

[230] *Id.* at 461.
[231] *Id.* at 462.
[232] *Id.*
[233] *NAACP v. Alabama*, 357 U.S. at 466.
[234] *See, e.g.*, Laird v. Tatum, 408 U.S. 1, 10, 13–14 (1972).
[235] *See id.* at 2.
[236] *Id.* at 13–14.
[237] *Id.* at 10.

media and publications in general circulation."[238] The Court also noted that

> some of the information came from Army Intelligence agents who attended meetings that were open to the public and who wrote field reports describing the meetings, giving such data as the name of the sponsoring organization, the identity of speakers, the approximate number of persons in attendance, and an indication of whether any disorder occurred.[239]

On these facts, the Court denied relief based on lack of standing, concluding that "[a]llegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm; 'the federal courts established pursuant to Article III of the Constitution do not render advisory opinions.'"[240]

Several points must be made about *Laird*'s significance for present-day questions of relational surveillance. First, it is important to note that the Court's decision was based on lack of standing; thus, the ultimate question of whether the Army's surveillance program violated the First Amendment was never answered.[241] The Supreme Court of California later noted this distinction in 1975, in *White v. Davis*, where it remanded for a hearing on the merits a case based on allegations of police undercover surveillance of activities of people affiliated with a university.[242] *Laird* was distinguished because standing in the case arose under California's provision for taxpayer suits.[243] Second, in determining the standing issue in *Laird*, the Court described its holding as "narrow" and found it "significant" that most of the information involved in the surveillance was publicly available from other sources.[244] In other words, the "mere existence" of the surveillance involved in *Laird* was truly "mere" as the Court saw it, and the harm alleged did not stem from the disclosure of individuals' membership in particular associations but simply from the presence of undercover Army operatives at

---

[238] *Id.* at 6.

[239] *Laird*, 408 U.S. at 6.

[240] *Id.* at 13–14 (quoting United Pub. Workers of Am. (C.I.O.) v. Mitchell, 330 U.S. 75, 89 (1947)).

[241] *See id.* at 15; *see also* White v. Davis, 533 P.2d 222, 226–27 (Cal. 1975) (noting that *Laird* was decided on standing grounds and that the Court "never reached the question of the constitutionality of the actual intelligence-gathering operation at issue").

[242] 533 P.2d at 224–27.

[243] *Id.* at 227.

[244] 408 U.S. at 6, 15.

public events.[245] Even in *Laird*, moreover, the Court was closely divided, with four justices dissenting.[246]

With respect to the standing issue, *Laird* may be usefully contrasted with the Court's 1976 decision in *Buckley v. Valeo*, where it upheld the compelled disclosure of certain campaign finance information, which necessarily entailed disclosure of political associations.[247] In so doing, the Court wasted little time in finding that the constitutional requirements of standing were fulfilled by the plaintiffs in the case, relying specifically on the fact that, in *NAACP v. Alabama*, "[t]his Court has held, for instance, that an organization 'may assert, on behalf of its members, a right personal to them to be protected from compelled disclosure . . . of their affiliation.'"[248] The Court made no particular inquiry into the level of harm anticipated by particular plaintiffs as a result of disclosure, apparently concluding that the requirement of disclosure itself was sufficient harm to support standing.[249]

Setting aside the question of standing, we now focus on the substantive question of when the government may inquire into citizens' protected associational activities. In *Buckley*, the issue most relevant for present purposes was whether certain requirements that campaign contributions be disclosed were an unconstitutional imposition on freedom of association, particularly for those who contributed to minority parties and those who contributed small amounts of money.[250] The Court affirmed the importance of freedom of association in the context of disclosure of associational membership, noting:

> We long have recognized that significant encroachments on First Amendment rights of the sort that compelled disclosure imposes cannot be justified by a mere showing of some legitimate governmental interest. Since *NAACP v. Alabama* we have required that the subordinating interests of the State must survive exacting scrutiny. We also have insisted that there be a "relevant correlation" or "substantial relation" between the governmental interest and the information required to be disclosed. This type of scrutiny is necessary even if any deterrent effect on the exercise of First Amendment rights arises, not through direct government action, but in-

---

[245] *See id.* at 10.
[246] *Id.* at 1.
[247] 424 U.S. at 63, 84.
[248] *Id.* at 12 n.10 (citing *NAACP v. Alabama*, 357 U.S. at 458).
[249] *See id.*
[250] *Id.* at 68–69, 83.

> directly as an unintended but inevitable result of the government's conduct in requiring disclosure.[251]

Significantly, the right to freedom of association was implicated by the *Buckley* disclosure requirements even though they applied not to official "membership" in an organization, but only to contributions to a candidate or political action committee.[252]

In *Buckley*, the Court went on to uphold the particular disclosure requirements at issue in light of the compelling government interests involved.[253] The Court recognized:

> It is undoubtedly true that public disclosure of contributions to candidates and political parties will deter some individuals who otherwise might contribute. In some instances, disclosure may even expose contributors to harassment or retaliation. These are not insignificant burdens on individual rights, and they must be weighed carefully against the interests which Congress has sought to promote by this legislation.[254]

In upholding the requirements nonetheless, the Court relied on the fact that those challenging the requirements had conceded that the disclosure requirements in general were the "least restrictive means" of advancing the substantial government interests in the "free functioning of our national institutions" addressed by the legislation and challenged the requirements only as they might apply to certain minority parties and candidates.[255]

The Court also noted that the allegations of harm due to disclosure were speculative and outweighed by the substantial public interest in the disclosures mandated by the law.[256] The Court left open the possibility, however, that sufficient evidence of potential harm might lead to a different result in future cases.[257] In particular, the Court opined that "[t]he evidence offered need show only a reasonable probability that the compelled disclosure of a party's contributors' names will subject them to threats, harassment, or reprisals from either Government officials or private parties."[258] In 1982, in *Brown v. Socialist Workers '74*

---

[251] *Id.* at 64 (citation omitted).
[252] *Buckley*, 424 U.S. at 65.
[253] *Id.* at 66–67.
[254] *Id.* at 68.
[255] *Id.* at 66–68.
[256] *Id.* at 71–72.
[257] *Buckley*, 424 U.S. at 71.
[258] *Id.* at 74.

Campaign Committee, the Court followed up on that possibility in the context of disclosures required by a state campaign finance law, concluding that the disclosure requirements were unconstitutional where the minor party involved presented "substantial evidence of both governmental and private hostility toward and harassment of SWP members and supporters."[259] The Court noted that "[t]he right to privacy in one's political associations and beliefs will yield only to a 'subordinating interest of the State [that is] compelling,' and then only if there is a 'substantial relation between the information sought and [an] overriding and compelling state interest.'"[260]

In considering whether compelled disclosure of association membership is permissible, the Supreme Court and lower courts following it have emphasized the extent to which the disclosure is tailored to the governmental objectives behind it.[261] When the required disclosure is too broad it is unconstitutional.[262] Thus, in 1960, in *Shelton v. Tucker*, the Court struck down a requirement that teachers list every organization to which they had belonged within the preceding five years, noting that "even though the governmental purpose be legitimate and substantial, that purpose cannot be pursued by means that broadly stifle fundamental personal liberties when the end can be more narrowly achieved."[263]

In 1978, in *Britt v. Superior Court*, the Supreme Court of California blocked a discovery request for disclosure of associational affiliations where the request was overly broad.[264] The request sought information related to the plaintiffs' involvement with "various organizations opposed to the . . . way in which the Port District operates its Airport."[265] In quashing the request, the court noted that the protections of freedom of association were not limited to membership in unpopular organizations, concluding that "[i]n view of the sweeping scope of the discovery order at issue, we think it clear that such order 'is likely to pose a substantial restraint upon the exercise of First Amendment rights.'"[266] In numerous other cases, courts have struck down requests

---

[259] 459 U.S. at 91 (citations omitted).
[260] *Id.* at 91–92 (citations omitted).
[261] *Buckley*, 424 U.S. at 64; Britt v. Superior Court, 574 P.2d 766, 768 (Cal. 1978).
[262] Shelton v. Tucker, 364 U.S. 479, 488 (1960); *Britt*, 574 P.2d at 777.
[263] 364 U.S. at 488.
[264] 574 P.2d at 775, 779.
[265] *Id.* at 769.
[266] *Id.* at 773 (quoting *White*, 533 P.2d at 232).

for disclosure of organizational membership that cut too broadly in relation to the government interests underlying the requests.[267]

In the discovery context, some courts have required an initial showing of "some probability" of First Amendment harm before shifting the burden to the requestor to establish that the requested information goes to the "heart of the matter" and that there is no other means for obtaining the necessary information.[268] Even those courts recognize, however, that concrete evidence of chilling effects is not necessary when a request is overly broad and that it is sometimes appropriate to use a "common sense approach" in assuming that disclosure of particular information will chill an association's First Amendment rights.[269]

When courts have permitted the compelled disclosure of associational membership, they have required a close connection between the required disclosure and the governmental purpose.[270] In an early case upholding a requirement "compelling organizations to register and to list their members on a showing merely that they are foreign-dominated and operate primarily to advance the objectives of the world Communist movement," for example, the Court noted that the requirement was narrowly limited to "organized groups which have been made the instruments of a long-continued, systematic, disciplined activity directed by a foreign power and purposing to overthrow existing government in this country."[271] Similarly, in a case upholding a subpoena to produce a membership list of a Ku Klux Klan group, the court noted the Klan's history of racially motivated violence and intimidation and the close connection of the context of the subpoena, which was the investigation of an arson in which Klan emblems were found on the lawn of the home that was burned, to the membership disclosure.[272]

---

[267] *See generally* Nat'l Commodity & Barter Ass'n v. Archer, 31 F.3d 1521 (10th Cir. 1994); Fed. Election Comm'n v. Hall-Tyner Election Campaign Comm., 678 F.2d 416 (2d Cir. 1982); Marshall v. Stevens People & Friends for Freedom, 669 F.2d 171 (4th Cir. 1981); Familias Unidas v. Briscoe, 619 F.2d 391 (5th Cir. 1980); Hastings v. N.E. Indep. Sch. Dist., 615 F.2d 628 (5th Cir. 1980); Int'l Union v. Garner, 102 F.R.D. 108 (M.D. Tenn. 1984); Pac.-Union Club v. Superior Court, 283 Cal. Rptr. 287 (Ct. App. 1991); Crocker v. Revolutionary Communist Progressive Labor Party, 533 N.E.2d 444 (Ill. App. Ct. 1988); Lubin v. Agora, Inc., 882 A.2d 833 (Md. 2005); Tilton v Moyé, 869 S.W.2d 955 (Tex. 1994); Right-Price Recreation, LLC v. Connells Prairie Cmty. Council, 21 P.3d 1157 (Wash. Ct. App. 2001).

[268] *E.g.*, Snedigar v. Hoddersen, 786 P.2d 781, 786 (Wash. 1990).

[269] *E.g.*, *id.* at 785 (citing authority).

[270] *Buckley*, 424 U.S. at 64; *see* Communist Party of the U.S. v. Subversive Activities Control Bd., 367 U.S. 1, 93 (1961).

[271] *Communist Party*, 367 U.S. at 81–82, 105.

[272] Marshall v. Bramer, 828 F.2d 355, 358, 360 (6th Cir. 1987).

Because of the important First Amendment rights implicated by disclosure of associational ties, the fact that the requested associational information is in third party hands does not remove the constitutional protection.[273] In 1983, in *In re First National Bank*, the U.S. Court of Appeals for the Tenth Circuit specifically distinguished the Fourth Amendment holding in *Miller* regarding financial records in third party hands "because the constitutionally protected right, freedom to associate freely and anonymously, will be chilled equally whether the associational information is compelled from the organization itself or from third parties."[274] This argument is particularly strong in today's society, where effective communication and association essentially requires the use of digital technology, which inevitably leaves records in third party hands. Whether or not these records are entitled to a reasonable expectation of privacy under the Fourth Amendment, they should not be available for the government to use to reconstruct protected associational membership lists.

The above cases make clear that, no matter how compelling the government interest, a broad-based request for lists of association membership, whether directed to an individual or to a third party, is unconstitutional unless the request is restricted to organizations directly implicated in the governmental purpose *and* obtaining the membership list is necessary to effectuating that purpose.[275]

---

[273] *See In re* First Nat'l Bank, Engelwood, Colo., 701 F.2d 115, 117–18 (10th Cir. 1983).

[274] *Id.*

[275] There is another potential source of constitutional limits on relational surveillance that is beyond the scope of the present Article. Due process may limit the extent to which, and purposes for which, governments may amass databases of personal information. *See* Slobogin, *Government Data Mining*, *supra* note 6, at 10. Though the Supreme Court has yet to strike down a government program on this basis, the Court has recognized the potential danger inherent in government aggregations of private data:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated pri-

IV. Freedom of Association for a Networked Society

Extensive government relational surveillance using network analysis data mining techniques poses a serious threat to liberty because of its potential to chill unpopular, yet legitimate, association, and also because of the chilling of legitimate association caused by possibly incorrect assessment of both legitimate and illegitimate associational membership. The potential for similar "guilt by association" to chill protected association is quite evident in the response to increased surveillance and targeting of Muslims and Arabs following the September 11, 2001 tragedy.[276] The danger is heightened in today's world wherein an increasing amount of communication is intermediated by third party service providers and more and more democratically significant association, assembly, and petition of the government is informal, emergent, and technologically mediated.[277] It is also clear that in this age of concern with international terrorism there will be growing pressure to apply network analysis techniques to root out terrorist and criminal activity, either because there is real potential for effective law enforcement and counterterrorism application or because of the inevitable lure of the chimerical "technological fix."

The First Amendment must supplement the Fourth Amendment and its related statutory scheme in regulating relational surveillance. The threat to freedom of association, especially with respect to new and empowering forms of association, is profound. Because the First Amendment is not grounded primarily in privacy and because it protects group membership data even when it is in third party hands, it plays a necessary part in limiting relational surveillance.[278]

The extension of First Amendment doctrine to relational surveillance is particularly appropriate because the First Amendment right to freedom of association has already been applied to regulate government access to associational information and that doctrine is instructive

---

vate data—whether intentional or unintentional—or by a system that did not contain comparable security provisions.

Whalen, 429 U.S. at 605–06 (footnote omitted).

Traffic data is certainly not the kind of paradigmatically intimate information involved in *Whalen v. Roe*. *See id.* Relational surveillance, however, has the potential to expose intimate associations and expressive associations which might be "potentially embarrassing or harmful if disclosed" so perhaps there is a cognizable due process issue. *See id.* Because the application of the First Amendment seems much more straightforward, I focus on it here.

[276] *See supra* note 11 and accompanying text.

[277] *See* US Const. amend I; *supra* notes 31–36 and accompanying text.

[278] *See In re* First Nat'l Bank, Engelwood, Colo., 701 F.2d 115, 117–18 (10th Cir. 1983).

in considering how to apply freedom of association doctrine to relational surveillance.[279] There is little precedent, however, in the First Amendment context for adapting to new technologies. Fourth Amendment doctrine, on the other hand, has repeatedly been adapted to evolving technological contexts.[280] Although the Fourth Amendment is not targeted to protect against relational surveillance, Fourth Amendment precedent is instructive as to how a First Amendment doctrine developed in the context of traditional associations should be adapted in light of technological evolution affecting associational behavior and surveillance methods. When adapted appropriately, the First Amendment's freedom of association guarantees place limits on relational surveillance that are not adequately reflected in current statutory or case law.

A. *The First Amendment Must Be a Primary Source of Protection Against Overreaching Relational Surveillance*

As the discussion in Part III.A demonstrates, present-day Fourth Amendment doctrine is not easily extended to cover relational surveillance using traffic data.[281] Because of the case law's crabbed approach to "reasonable expectations of privacy," which are destroyed by disclosure to third party intermediaries, and surveillance law's emphasis on protecting content and guarding against real-time interception, there are difficult arguments to be made in bringing network analysis of traffic data within the ambit of the Fourth Amendment's protections.

One way to deal with this conundrum might be to view the Fourth Amendment through a special First Amendment lens in cases implicating expressive activity. The extent to which and the way in which the First and Fourth Amendments combine to regulate government activity is unclear, as recently discussed by Professor Daniel Solove, who argues generally that the First Amendment has a role to play in regulating surveillance.[282] A general framework for analyzing the constitutionality of government acquisition of information about First Amendment activity has not yet been established, but freedom of speech concerns do underlie certain restrictions courts have placed on government acquisition of information.[283] For example, the distinction between content of

---

[279] *See* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958).

[280] *See* Kyllo v. United States, 533 U.S. 27, 29–30 (2001) (thermal imaging device); Katz v. United States, 389 U.S. 347, 348 (1967) (electronic listening and recording device).

[281] *See supra* notes 121–170 and accompanying text.

[282] *See* Solove, *supra* note 9, at 128–33.

[283] *Id.* at 157–61, 176–77.

communications and traffic data is arguably undergirded by First Amendment concerns. Moreover, the First Amendment dictates that Fourth Amendment procedures, including the standard for particularity of warrants, must be applied with "scrupulous exactitude" when seizing books and other First Amendment-protected materials.[284] As Solove points out, however, the case law does not resolve the question of what to do when government information gathering has First Amendment implications yet falls outside of the Fourth Amendment because there is no "reasonable expectation of privacy" in the information under present Fourth Amendment doctrine.[285]

As part of a general attack on current Fourth Amendment doctrine, Professor Akhil Amar has argued that the permissibility of a search under the Fourth Amendment should be determined by a general inquiry into reasonableness and that the First Amendment significance of the information acquired should inform the reasonableness of a search under the Fourth Amendment.[286] Solove suggests that whether a search "implicates" the First Amendment should be an alternative to the "reasonable expectation of privacy" threshold under current Fourth Amendment doctrine.[287] As another alternative, Solove suggests that the First Amendment should "provide an independent source of criminal procedure" under a general framework involving a two-part inquiry into whether the activity falls within the boundaries of the First Amendment and whether the government information gathering has a chilling effect upon the First Amendment activity.[288]

The awkward fit between freedom of association's interest in protecting a varied and lively civic square—and hence in protecting unpopular and fringe associations—and the Fourth Amendment's "reasonable expectations of privacy" suggests that merely using the First Amendment as a trigger or booster for Fourth Amendment scrutiny will not be sufficient to serve the distinctive interests in freedom of association implicated by relational surveillance. A direct resort to the First Amendment, in addition to any appropriate Fourth Amendment analysis, is needed. Moreover, in this specific context, there is no need to create a framework for applying the First Amendment to govern-

---

[284] Zurcher v. Stanford Daily, 436 U.S. 547, 564 (1978); Stanford v. Texas, 379 U.S. 476, 485 (1965).

[285] Solove, *supra* note 9, at 132.

[286] Akhil Reed Amar, *Fourth Amendment First Principles*, 107 Harv. L. Rev. 757, 804–06 (1994).

[287] Solove, *supra* note 9, at 132.

[288] *Id.*

ment acquisition of information out of whole cloth. Existing case law tells us much about how to evaluate the constitutional permissibility of government attempts to obtain associational information.[289] Freedom of association doctrine tells us that government inquiry into membership in expressive associations must be driven by a compelling government interest and that there must be a substantial relation between the specific disclosure and that interest.[290] Where the inquiry is too broad, even where the associations involved are not particularly unpopular or disfavored, courts can employ a "common sense" presumption that there will be an impermissible burden upon freedom of association.[291] In what follows, this Article therefore considers how the First Amendment, as interpreted in light of modern technology, might serve as an independent source of limitations on relational surveillance.

B. *Principles for Technological Adaptation Derived from Fourth Amendment Law*

Although the prospects for direct Fourth Amendment protection from relational surveillance seem rather bleak at this point, the ways in which more traditional Fourth Amendment doctrine has been adapted to deal with advancing technology provide clues about how to adapt freedom of association protection in the face of technological advance. Fourth Amendment doctrine has often focused on how to adapt constitutional protections to new technological realities.[292] In this respect, freedom of association doctrine lags behind. Case law to date essentially deals exclusively with membership lists (or lists of contributors) compiled by formal, traditional organizations and obtained directly from those organizations.[293] What should be done when technology shifts the locus of important associational activity away from traditional organizations and the means of data acquisition away from traditional requests for documents and lists? The ways in which Fourth Amendment doctrine has adapted to technological change provide principles that can inform the extension of freedom of association doctrine to new technological circumstances.

---

[289] *See supra* notes 227–275 and accompanying text.

[290] Buckley v. Valeo, 424 U.S. 1, 64 (1976); Shelton v. Tucker, 364 U.S. 479, 488 (1960); Britt v. Superior Court, 574 P.2d 766, 768, 777 (Cal. 1978).

[291] *See* Snedigar v. Hoddersen, 786 P.2d 781, 785 (Wash. 1990).

[292] *See, e.g.*, *Kyllo*, 533 U.S. at 29–30 (thermal imaging device); *Katz*, 389 U.S. at 348 (electronic listening and recording device).

[293] *See supra* notes 227–275 and accompanying text.

Three specific principles are relevant here: First, surveillance doctrine must be responsive to technological change that transforms the *situs* of private communication. Second, surveillance doctrine must recognize that new means of analyzing available data change the constitutional balance. Finally, surveillance doctrine must be sensitive to the extent to which a particular search technology discriminates between innocent and illegal behavior.

1. Surveillance Doctrine Must Respond to Destabilizing Technical Change that Transforms the *Situs* of Private Communication

The seminal case for modern Fourth Amendment law is *Katz v. United States*, decided by the Supreme Court in 1967.[294] In *Katz*, the Court considered the constitutionality of a search that involved attaching an electronic listening device to the outside of a telephone booth and listening to the occupant's end of telephone calls.[295] In evaluating the Fourth Amendment claim, the Court made its now famous statement that

> the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[296]

The Court rejected an analysis based on the extent to which the surveillance method intruded upon a "constitutionally protected area."[297] Instead, the Court relied on the phone booth occupant's intent to exclude the "uninvited ear" and stated that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[298] The Court's holding in *Katz* recognized the need for surveillance doctrine to adapt to technology-driven social change. Given that individuals increasingly held private conversations by telephone and that telephone booths were designed to facilitate such private conversations away from the home, the Court concluded that it would be unreasonable to permit government surveillance of such conversations without a warrant.[299]

---

[294] *See generally* 389 U.S. 347.
[295] *Id.* at 348.
[296] *Id.* at 351 (citations omitted).
[297] *Id.*
[298] *Id.* at 352.
[299] *Katz*, 389 U.S. at 352.

Just as the telephone had become such an indispensable means of communication at the time of the *Katz* decision, the Internet and other forms of digital communication have taken on a critical communication role in today's society.[300] The locus of critical associational activity has moved. Surveillance law must adapt so that freedom of association remains protected under these new social and technological circumstances. The protection of association mediated by digital technology is just as important as the protection of traditional organizations, and relational surveillance has the same potential to suppress expressive association as direct requests for membership lists.

2. Surveillance Doctrine Must Recognize that New Means of Analysis of Available Data Can Change the Constitutional Balance

In 2001, in *Kyllo v. United States*, the Supreme Court dealt not with a change in the technology of constitutionally protected activity, but with a change in the technology of surveillance, which permitted what was effectively a search of a home using data acquired without ever going onto the premises.[301] The Court held that the development of thermal imaging technology required an expansion of the scope of Fourth Amendment coverage such that

> obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.[302]

The Court specifically acknowledged that "[t]he question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[303]

This emphasis on the need to reevaluate the scope of constitutional protection in light of advancing technology is directly relevant to considering whether the Constitution protects against data mining and network analysis technology. Like the thermal imager in *Kyllo*, data

---

[300] *See id.*

[301] 533 U.S. at 29–30.

[302] *Id.* at 34 (citations omitted).

[303] *Id.*

mining takes data that is already accessible to law enforcement (the heat radiating from the house was in "plain view") and transforms it into new knowledge that would not otherwise be available by constitutional means.[304] In the case of relational surveillance of traffic data, network analysis produces knowledge which, like the thermal image in *Kyllo*, is embedded in the data, yet not available without applying the technology.[305] The Court in *Kyllo* specifically rejected the proposition that an investigating tool that was a means of processing data rather than collecting it could not constitute a search.[306] The dissent emphasized the collection of the data about heat emanating from a dwelling, analogizing it to the smell of smoke and arguing that it was ridiculous to provide protection for data that is so obviously available in "plain view."[307] In so doing, the dissent did not incorporate data *analysis* into its definition of the search, arguing that the production of a thermal image was merely an "inference" from data in plain view.[308] The Court rejected this argument, holding that the fact that an "inference" was involved did not insulate an investigative technique from Fourth Amendment review.[309]

Advances in surveillance technology are of two types: finding ways to obtain more data and finding ways to obtain more information from available data. The recognition that a technology for analyzing available data can tip the constitutional balance is a critical bulwark against the potential for advancing technology to undermine constitutional norms.

3. Surveillance Doctrine Must Be Sensitive to the Extent to Which a Particular Search Technology Discriminates Between Innocent and Illegal Behavior

Notwithstanding *Kyllo*'s dictates about the application of technological means of investigation, there are technological means not in "general public use," the use of which do not constitute a Fourth Amendment search.[310] In 2005, in *Illinois v. Caballes*, the Court considered the constitutionality of a suspicionless "dog sniff" for illegal drugs

---

[304] *See id.*

[305] *See id.*

[306] *Kyllo*, 533 U.S. at 35–36.

[307] *Id.* at 42–44 (Stevens, J., dissenting).

[308] *See id.* at 41.

[309] *Id.* at 36 (majority opinion).

[310] *Compare* Illinois v. Caballes, 543 U.S. 405, 409–10 (2005) (drug sniff by police dog not a search), *with Kyllo*, 533 U.S. at 34 (thermal imaging is a search).

during a routine traffic stop.[311] The Court held categorically that the "dog sniff" did not constitute a search because "governmental conduct that *only* reveals the possession of contraband 'compromises no legitimate privacy interest.'"[312] The Court contrasted the "dog sniff" with the thermal imaging in *Kyllo*, noting that "[c]ritical to [the *Kyllo*] decision was the fact that the device was capable of detecting lawful activity."[313] Regardless of whether the Court was correct in assuming that dog sniffs are sensitive only to the presence of contraband (an assumption strongly disputed by Justice Souter in dissent),[314] the important point remains: the intrusiveness of a particular form of technological surveillance depends on the extent to which it exposes both legitimate and illegitimate activity and its accuracy in distinguishing the two.[315]

C. *Adapting First Amendment Freedom of Association to New Technologies*

1. Establishing a Freedom of Association Framework for Evaluating Relational Surveillance

The three principles identified from the path that Fourth Amendment doctrine has trod in adapting to technological change can be helpful in thinking about how to update First Amendment doctrine in the context of modern day relational surveillance. First, just as technological advances expanded the *situs* of private life to include telephone booths, communications technology developments have affected the *situs* of associational life.[316] Traditional, formal associations with hierarchical means of promulgating policy positions and well-defined memberships persist, but an increasingly large proportion of socially significant expressive association takes place in informal, emergent groups, the membership of which may not be known to anyone. Traditionally, freedom of association protections have been extended only to intimate associations and to associations engaged in expressive activities, though those expressive activities are very broadly defined.[317]

---

[311] *See Caballes*, 543 U.S. at 407; *see also* United States v. Place, 462 U.S. 696, 697 (1983).

[312] *Caballes*, 543 U.S. at 408 (citations omitted).

[313] *Id.* at 409.

[314] *Id.* at 410–13 (Souter, J., dissenting).

[315] *See id.* at 409–10 (majority opinion).

[316] *See Katz*, 389 U.S. at 353.

[317] Boy Scouts of Am. v. Dale, 530 U.S. 640, 655 (2000) ("[A]ssociations do not have to associate for the 'purpose' of disseminating a certain message in order to be entitled to the protections of the First Amendment. An association must merely engage in expressive activity that could be impaired in order to be entitled to protection.").

Under traditional circumstances, it was possible to determine whether an association was engaged in expressive activities before determining whether to enforce a request for disclosure of a membership list.[318] Because network analysis discloses membership simultaneously with identifying associations, waiting until an association is identified as "expressive" in nature before determining whether it is protected from disclosure of its membership is no longer possible.

The inquiry therefore must focus not on whether a specific association is "expressive," but on the likelihood that a particular instance of relational surveillance will disclose membership in expressive associations. Such an approach is grounded in the well-established inquiry into First Amendment statutory overbreadth—whether "rights of association were ensnared in statutes which, by their broad sweep, might result in burdening innocent associations."[319] Assessment of the likelihood of burdening expressive association must be made in light of the very broad definition of expressive association set forth by the Supreme Court in 2000, in *Boy Scouts of America v. Dale*.[320] Just as courts sometimes make a common sense assumption that a broad disclosure of associational memberships will result in a reasonable probability of chilling of protected association,[321] courts should assume that a social network analysis of traffic data will reveal the membership and structure of expressive associations, among others, unless the analysis procedure is sufficiently narrowly targeted.

Second, even when some data has already been disclosed or is in third party hands, First Amendment protections must be extended to government use of sophisticated technological means, such as network analysis algorithms, which evade traditional prohibitions on compelling disclosure of associational information yet produce equivalently intrusive information. The use of sophisticated network analysis algorithms to uncover associations is not like the surveillance upheld by the Court in 1971, in *Laird v. Tatum*, which focused on publicly available information and attendance at meetings open to the public.[322] The associational information derived from network analysis of traffic data is not

---

[318] *See id.* at 656.

[319] Broadrick v. Oklahoma, 413 U.S. 601, 612 (1973) (citing United States v. Robel, 389 U.S. 258 (1967); Keyishian v. Bd. of Regents, 385 U.S. 589 (1967); Aptheker v. Sec'y of State, 378 U.S. 500 (1964); *Shelton*, 364 U.S. 479); *see also* Lynch, *supra* note 9, at 277–78 (discussing the applicability of First Amendment overbreadth doctrine in the surveillance context); Solove, *supra* note 9, at 158–59.

[320] *See* 530 U.S. at 655.

[321] *See Snedigar*, 786 P.2d at 785.

[322] *See* 408 U.S. 1, 6 (1971).

apparent in the raw data. Although the associational information may be implicit in available traffic data, just as thermal images are implicit in the measurement of thermal emissions from a home, the use of network analysis algorithms is an additional, constitutionally cognizable intrusion.[323] The correlations uncovered by network analysis are quite unlike the simple lists of numbers called or financial transactions associated with a particular account involved in *Smith v. Maryland* or *United States v. Miller*.[324] Communications intermediaries would not be able to "see" these implicit structures in the ordinary course of business while using traffic data either to transmit communications or in conjunction with administrative functions such as billing. Indeed, the pseudonymous and nonhierarchical nature of emergent association means that there may be no one—not even the participants in the association themselves—who has a list of participants in a particular emergent association until a network analysis is performed.

Third, the extent to which surveillance intrudes upon constitutionally protected freedoms depends heavily on a specific program's ability to distinguish legal from illegal behavior.[325] This means that the extent to which a particular instance or program of relational surveillance burdens protected association depends on the likelihood that legitimate expressive associations will be exposed to government scrutiny. That likelihood depends both on the accuracy of the technology used to distinguish suspect from legitimate associations and on the potential for abuse of the technology and relevant data by those with access to it. Whether a network analysis technology intrudes on protected freedom of association should be judged at the outset by its ability to distinguish those associations that are relevant to the compelling government interest that motivates the analysis from other associations and to refrain from revealing the membership of associations that are not closely related to the government purposes at issue. It should also be judged by its susceptibility to misuse as a means to target unpopular organizations or political opponents. When a particular technique is likely to disclose a significant amount of protected activity or is inaccurate in its assessment of traffic data, there is a similarly significant likelihood of burdening freedom of association.

In sum, the questions to pose in evaluating the constitutionality of relational surveillance based on computerized network analysis of traffic

---

[323] *See Kyllo*, 533 U.S. at 35–37.

[324] *See* Smith v. Maryland, 442 U.S. 735, 736 n.1 (1979); United States v. Miller, 425 U.S. 435, 436 (1975).

[325] *See Caballes*, 543 U.S. at 408–10.

data should be these: Does the surveillance serve a legitimate and compelling government interest? Is the analysis sufficiently accurate and narrowly tailored to that interest in light of the extent to which it is likely to expose protected expressive and intimate associations? The next Section discusses how particular forms of relational surveillance implicate the First Amendment's freedom of association requirements.[326] How to implement this standard in a practical manner is, of course, the rub. This Article has focused primarily on identifying the issue with the hope that the Constitution's mandate to protect expressive association even in a networked world will take a more prominent place in the ongoing debate about surveillance regulation. The next Section attempts to sketch out how these requirements might be enforced.

2. Applying the Freedom of Association Framework to Network Analysis

The extent to which network analysis implicates the right to freedom of association depends on the type of analysis. The following Subsections explain how freedom of association is likely to be implicated in the three types of analysis identified in Part II.[327] Of course, a particular surveillance program may overlap these paradigmatic examples.

a. *Analysis of Known Social Networks*

Where social network analysis is used to understand relationships between a group of already-identified individuals, the freedom of association question depends almost entirely on how and why the individuals were identified. Professor Linda Fisher has argued, in the more general context of real world political surveillance and expressive association, that the First Amendment would be satisfied by a threshold of reasonable suspicion that a group is involved in criminal activity and by a requirement that the least restrictive means of investigation be used.[328] Perhaps some similar threshold would be appropriate in the context of employment of social network analysis to investigate the structure of a known group. It would be inappropriate, for example, for the government to obtain call traffic records of the members of a legitimate political or religious group so as to engage in an investigation of its leadership structure. Such an analysis serves no legitimate and

---

[326] *See* Solove, *supra* note 9, at 159–76 (offering a general proposal about how to implement First Amendment limitations on surveillance).

[327] *See supra* notes 77–116 and accompanying text.

[328] *See* Fisher, *supra* note 11, at 627–28.

compelling government interest and implicates freedom of association concerns in much the same way as, though perhaps to a lesser extent than, a compelled disclosure of a membership list.[329] On the other hand, there might be legitimate reasons (including, for example, research) for government to conduct a similar network analysis of an expressive association using publicly available information about relationships. Although one can imagine unsavory government uses of social network analysis of known groups using publicly available data, it is hard to argue that the potential for such an analysis would have a serious chilling effect on protected association.

Just as government agents could presumably piece together a list of group members from publicly available sources without running afoul of freedom of association strictures, it would seem that the freedom of association threshold for uses of social network analysis to study known groups should lie at government acquisition of nonpublic communications records from communication intermediaries. Some showing of likelihood that the group is engaged in criminal or terrorist activities should be required for such acquisition in order to demonstrate the requisite government interest in the analysis. Because the intrusion on expressive association is relatively minimal given that group members have already been identified, the reasonable suspicion threshold suggested by Fisher seems appropriate here as well.[330]

b. *Targeted Link Analysis*

As described in Part II, targeted link analysis can be employed to investigate the associations surrounding a particular individual or group of individuals who have aroused suspicion in some other way.[331] Essentially, a targeted link analysis can produce information regarding the target individual equivalent to the list of group memberships required by the statute struck down by the Supreme Court in 1960, in

---

[329] *See NAACP v. Alabama*, 357 U.S. at 460–62.

[330] *See* Fisher, *supra* note 11, at 627–28. For a general argument that under the Fourth Amendment the threshold for search should be on a sliding scale based on the level of intrusion, see Slobogin, *Let's Not Bury* Terry, *supra* note 126, at 1066–70. The First Amendment requires a similar tailoring of the level of impact on the right to freedom of association to the extent to which the surveillance furthers a compelling government interest. *See Dale*, 530 U.S. at 648; Communist Party of the U.S. v. Subversive Activities Control Bd., 367 U.S. 1, 93 (1961) (distinguishing prior case law based on the magnitude of the governmental interest at stake in the case and the extent to which the registration and disclosure provisions were tailored to serve that interest).

[331] *See supra* notes 82–93 and accompanying text.

Shelton v. Tucker.[332] Like such an indiscriminate request for information about group memberships, a targeted link analysis is very likely to expose a wide range of expressive and intimate associations to government scrutiny. Thus, such an analysis runs afoul of the First Amendment unless it is properly justified and narrowly tailored.[333]

Current surveillance regulation does not adequately account for the imposition on freedom of association which targeted link analysis entails. As discussed above, the Supreme Court has held, based on the third party doctrine, that the Fourth Amendment does not protect lists of phone numbers called by individuals.[334] Lower courts have extended this holding to similar electronic traffic data used by ISPs.[335] Obtaining communications traffic data in real time is currently regulated by "pen register" statutes, which permit traffic surveillance as long as the government certifies that "the information likely to be obtained . . . is relevant to an ongoing criminal investigation."[336] Obtaining stored traffic data currently requires a similar, or even lesser, showing.[337]

The First Amendment, however, mandates a higher threshold for targeted link analysis.[338] A link analysis can be the equivalent of disclosing a large fraction of an individual's group affiliations, much as was demanded of teachers by the statute struck down in *Shelton*.[339] Such a wide-ranging inquiry into an individual's associations is precluded unless First Amendment standards are met.[340] Moreover, because link analysis employs second and even higher order connections (i.e. the links between the central individual's associates, the links between their associates, and so forth) to categorize an individual's associates into groups and to determine such things as the structure of a group or a particular individual's role in the group, it is not only more intrusive to the central individual than a mere list of direct links or numbers dialed, but also intrudes into the associations of untargeted individuals.

---

[332] *See Shelton*, 364 U.S. at 487–88.

[333] *See id*.

[334] *Smith*, 442 U.S. at 745–46.

[335] United States v. Forrester, 500 F.3d 500, 509–10 (9th Cir. 2008); United States v. Hambrick, No. 99-4793, 2000 U.S. App. LEXIS 18665, at *11–12 (4th Cir. Aug. 3, 2000).

[336] 18 U.S.C. § 3122 (2000).

[337] *See* 18 U.S.C.A. § 2703 (West 2000 & Supp. 2007) (requiring stored data to be "relevant and material to an ongoing investigation"); 50 U.S.C.A. § 1861 (West 2003 & Supp. 2007) (requiring a showing that the stored data is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities").

[338] *See Shelton*, 364 U.S. at 488.

[339] *Id.*

[340] *Id.*

The First Amendment does not call for a categorical ban on targeted link analysis, but rather for its judicious use. The fact that link analysis begins with specific identified individuals means that the government frequently may be able to meet the First Amendment's requirements of narrow tailoring to a compelling government interest, at least with respect to the associations of the target individual.[341] If there is probable cause to believe that the target individual has committed a crime or is engaged in terrorist activity, a link analysis is certainly appropriate. The broad sweep of such an analysis, however, means that a mere relevance standard for obtaining the necessary traffic data cannot provide the narrow tailoring required by strict scrutiny either for the central individual or for the other individuals caught up in the web of associational links.

How should targeted link analysis be regulated so as to comport with the First Amendment's strictures? As a practical matter there must be a workable framework within which law enforcement officials can operate. Though it would be possible to develop a separate First Amendment standard to govern acquisition of traffic data for link analysis, it may be sufficient to import existing standards used in the Fourth Amendment context, at least as a baseline.[342] Such an approach, if implemented so as to accord with First Amendment requirements, would have many practical advantages because it would not require law enforcement officers to learn an entirely new lexicon of standards.

In the context of targeted link analysis, the greatest potential burden on protected association would fall on the target individual, because the goal of the analysis would be to get a complete picture of that individual's associations. As in *Shelton*, such a burden cannot be justified without a close relationship between that individual's associations and a compelling government interest such as fighting serious crime or thwarting terrorism.[343] Before undertaking that kind of an analysis, law enforcement officials should be required to demonstrate such a relationship. One way to ensure such a substantial relationship with respect to the target individual would be to require a warrant based on probable cause either that the individual who is the focus of a link analysis has committed a crime to which his or her associations are relevant or that he or she is involved in a terrorist or criminal enterprise. To ensure a substantial relationship between the inquiry into

---

[341] *See Buckley*, 424 U.S. at 64; *NAACP v. Alabama*, 357 U.S. at 460–63; *Britt*, 574 P.2d at 768.

[342] *See* Solove, *supra* note 9, at 161–62.

[343] *See* 364 U.S. at 488.

associations and a compelling government interest, the crime involved should also be of a sufficient degree of seriousness.

A more difficult question is what standard to require for obtaining the communications traffic records of those associated with an individual who is the focus of a link analysis. Network analysis uses these second and higher order links to determine the nature of the target individual's associations with more accuracy. For example, a suspected terrorist may communicate with three groups of people—his family, a church group, and a terrorist organization. There may be no way to distinguish the members of these groups based on the target's traffic data records alone. If one obtains traffic data related to all of that central individual's contacts and perhaps even of their contacts, however, it may be possible to separate these three groups. Family members may all contact one another, but only the central individual contacts both family members and members of the terrorist organization, and so forth. Of course, the analysis may not always be cut and dried—different groups may have overlapping memberships—but the point remains that the more connection data obtained, the more accurate a link analysis is likely to be in separating out the various groups to which the target individual belongs.

For this reason, obtaining the traffic records of an individual who has been linked to a suspected criminal or terrorist has an ambiguous effect on that individual. The records may serve either to exonerate that individual or to tie him or her more closely to the focus of the analysis. Moreover, the use of one individual's traffic data in conjunction with a link analysis focused on another is unlikely to reveal the broad sweep of that second individual's associations. Thus, the burden on the freedom of association of such secondary individuals is significantly less than would be imposed by a wide-reaching inquiry into that individual's associations.

On the other hand, because a link analysis will tend to be improved in its accuracy by including more and more data about these higher order associations, a standard of mere "relevance," such as applies to most traffic data today, could be interpreted so as to permit intrusions into the associations of a very large number of innocent individuals with only tenuous connections to the target individual.[344] This is particularly true because the structure of social networks is usually quite densely connected, perhaps even with a "small world"

---

[344] *See* 18 U.S.C.A. §§ 2703, 2709 (West 2000 & Supp. 2007); 50 U.S.C.A. § 1861 (West 2000 & Supp. 2007).

property.[345] This means that going just a few links out from any particular individual is likely to sweep in a large number of others. Innocent expressive associations of such related individuals will unavoidably be exposed by the link analysis. The more attenuated the links to the target individual become, the less likely it becomes that traffic data about these tenuously connected individuals will be of sufficient use in sorting out the associations of the target person to justify the burden on association of those individuals.

Obtaining the traffic data records of those who are not targets should therefore be regulated according to a balance between relevance to the link analysis and the degree of imposition on associational rights. A standard of reasonable suspicion that the second individual is a member, along with the target of the link analysis, of a criminal or terrorist enterprise might be appropriate. Given the probable cause standard for initiating the link analysis (and in the absence of supplemental information to the contrary) this standard is likely to be met for many of those with some degree of first order connection to the target individual. On the other hand, imposing even a reasonable suspicion threshold to obtain the traffic data of those with first-order relations to the target individual might seriously hamper the network analysis, and might even make it harder to exonerate those with innocent connections to the target individual. As an alternative, it might be reasonable to permit government officials to obtain traffic records for anyone directly connected to the target individual and then impose a reasonable suspicion threshold for those with more remote connections, where information developed from the analysis of first and second-order links could be used as part of the grounds for reasonable suspicion. Any such threshold is less and less likely to be met (unless further information is developed based on the earlier analysis) with respect to those more tenuously linked to the target individual, but the records of these individuals are also decreasingly likely to be important for the network analysis.

c. *Pattern-Based Network Analysis*

May the government constitutionally employ a broad-based network pattern analysis technique to identify suspicious groups? Assume for present purposes that a compelling government interest, such as prevention of terrorism, motivates the surveillance. The constitutional-

---

[345] *See* BARABÁSI, *supra* note 7, at 41–54 (discussing the "small world" problem); WATTS, *supra* note 7, at 37–42 (same).

ity of the program thus depends on the extent to which the pattern analysis is tailored to that interest in light of the extent to which it is likely to burden protected expressive associations.[346] Answering this question depends critically on the accuracy of the pattern analysis algorithm and its ability to discriminate between associations relevant to the compelling government interest and other associations. The ability of a network analysis algorithm to identify a particular type of organization depends first on having either sufficient examples of traffic data associated with the particular type of association at issue—a terrorist organization, for example, or an association of pedophiles—or a sufficiently accurate model of the communication patterns of such organizations to generate a pattern that can be "matched" against available traffic data. Second, the pattern must be sufficiently unique and well specified that it will not "match" large numbers of other types of associations—book groups, political organizations, and so forth.

Underlying any such pattern matching analysis is an assumption that there is a sufficiently unique pattern to be found. If, for example, book groups and terrorist organizations (or, perhaps, radical political organizations and terrorist organizations) have similar traffic data patterns, no network analysis algorithm will ever distinguish them using that data. Any attempt will be overinclusive. If, on the other hand, various terrorist organizations have significantly different traffic data patterns, an attempt to identify them by such patterns will be underinclusive. Social network analysis is still in its infancy. It is highly unlikely at this point that a pattern-based analysis of traffic data could be sufficiently well tailored to identify a particular type of illegitimate organization as distinguished from numerous legitimate organizations. This is particularly true with respect to organizations, such as terrorist networks, which are, thankfully, sufficiently rare as not to have been studied in detail in any statistically relevant numbers. The potential overbreadth of such a pattern-based analysis of associations, its likely inaccuracy, and its Orwellian potential to chill legitimate association makes it extremely unlikely that First Amendment standards could be met.[347]

---

[346] *See Shelton*, 364 U.S. at 488.

[347] This analysis suggests why the Fourth Amendment alone is insufficient to protect the freedom of association interests implicated by pattern-based analysis. An empirical survey of perceived intrusiveness ranked data mining of phone, credit card, and travel records as less intrusive on average than a pat-down search and slightly more intrusive than an "ID check and questioning during a brief stop," suggesting to the author of the study that a reasonable suspicion standard would be appropriate for this kind of "event-driven data mining." Slobo-

That being said, it may be possible in theory to develop pattern-based relational analysis techniques, perhaps in combination with mining of transactional data,[348] which would be sufficiently accurate to meet the First Amendment standard. Therefore, rather than categorically rule out the possibility of pattern-matching network analysis (which is unlikely to happen in any event as long as there is some hope that it can expose terrorist organizations before they strike), such programs must be subject to judicial and congressional scrutiny. Pattern-based relational surveillance is unlike many other surveillance techniques in that its effectiveness is much less likely to be significantly reduced by disclosure—even if the specific algorithms are disclosed. Unlike an individual "profile," which might be manipulated once it is publicized, a network analysis deals with patterns of communications among a group of individuals. If such a pattern is truly characteristic of a particular type of illegitimate association as distinct from other, legitimate organizations, it is likely to be very difficult for that organization to manipulate. Patterns of communication arise because they are useful—perhaps even essential—to a group's activities. If exposing that the government is looking for a particular "terrorist" communication pattern forces malevolent organizations to adopt other, presumably less effective and riskier, communication patterns in order to "blend in" or deters such groups from acting at all, that, in itself, could be the greatest success of a pattern-based analysis scheme.

Because pattern-based network analysis cannot meet First Amendment standards at present (and may be inherently unable to do so), there is no legitimate need for government acquisition of large and indiscriminate databases of communications records, such as the alleged acquisition by the NSA under the Bush administration of AT&T's call record database.[349]

---

gin, *Government Data Mining*, *supra* note 6, at 18, 21 tbl. The average viewpoint about the intrusiveness of a particular type of "dataveillance" may be relevant for assessing "reasonable expectations of privacy," but it is assuredly not the touchstone for First Amendment analysis, which seeks to protect unpopular, out of the mainstream expression.

[348] Such an approach may or may not be feasible in practice, even if all data were available. Some researchers argue that loose social networks, such as terrorist networks in an emergent rather than top-down fashion might be complex systems, which are inherently unpredictable in detail (except during the very last stages of implementing a specific plan of action). *See* Aaron B. Frank & Desmond Saunders-Newton, *Journey from Analysis to Inquiry: Technology and Transformation of Counter-Terrorism Analysis*, *in* Emergent Information Technologies, *supra* note 6, at 315, 320–24; Mark Lazaroff & David Snowden, *Anticipatory Models for Counter-Terrorism*, *in* Emergent Information Technologies, *supra* note 6, at 51, 69–71.

[349] *See* Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 978 (N.D. Cal. 2006).

3. Freedom of Association and Access to Communications Traffic Data Outside of the Context of Network Analysis

As discussed above, freedom of association demands a stricter standard for acquisition and use of traffic data for network analysis than is reflected in the current statutory regime.[350] But what of government acquisition of traffic data for use in more traditional investigations? A list of an individual's first order communications traffic data certainly has some potential to burden expressive association even though the list may not be equivalent to a broad disclosure of association memberships. Moreover, in some cases the burden may be quite great (consider the case, discussed by Solove, where the phone data pertains to the office phone of an unpopular expressive association, for example, or the case where the traffic data discloses repeated contacts by an individual with an unpopular expressive association).[351] The First Amendment balance suggests that where there is an evident potential to burden expressive association, a probable cause warrant should be required. In other cases, at a minimum, a court order should be required to obtain traffic data so that a neutral judge can assess the potential First Amendment burdens. In determining whether to grant an application for such an order, courts should be directed to consider the potential burden on protected association and not simply whether the investigation is "conducted solely upon the basis of activities protected by the first amendment to the Constitution."[352] That standard, currently enshrined in FISA, is utterly insufficient under the First Amendment.[353] Applicants for such orders should be required to articulate specific facts based upon which the court can assess the First Amendment issues.

D. *Enforcing Freedom of Association Rights in a Networked Society*

Even if we are convinced that government surveillance of traffic data implicates freedom of association rights under the First Amendment, there remains the question of how to enforce such rights as a practical matter. Here we come up against several difficulties. First, because network analysis does not in most cases begin by targeting expressive or intimate associations, the proof of First Amendment

---

[350] *See supra* notes 208–275 and accompanying text.

[351] *See* Solove, *supra* note 9, at 169.

[352] *See* 18 U.S.C.A. § 2709 (West 2000 & Supp. 2007); 50 U.S.C.A. §§ 1842, 1861 (West 2003 & Supp. 2007).

[353] *See* 50 U.S.C. §§ 1842, 1861.

harm in these contexts will nearly always depend on an overbreadth argument, such as that made in *Shelton*.[354] Chilling effects are difficult to prove directly except in egregious cases. Second, the surveillance context, along with the national security implications of network analysis, mean that it will be difficult even to determine what law enforcement agencies are doing with respect to network surveillance, as is illustrated by the cases involving the NSA programs, which depended on a whistleblower and media investigations for the basic factual allegations.[355] Third, network analysis is technically complicated and, particularly for pattern-based analysis, assessing its accuracy requires technical information about the algorithms and models employed, which governments will resist disclosing for both good and nefarious reasons. Finally, as discussed above, there are hurdles to establishing standing in a lawsuit based on freedom of association, at least under the federal associational guarantee.[356] These difficulties are exacerbated in a surveillance situation where it is hard to know what kinds of analysis the government is employing and who is being targeted. Despite the difficulties, the importance of free association to democratic life demands that we seek ways to regulate relational surveillance adequately. This Section considers how that might be done.

1. Civil Lawsuits Challenging Relational Surveillance

The main hurdles to effective civil lawsuits challenging unconstitutional relational surveillance are learning about unconstitutional activities and establishing standing to sue. Both targeted link analysis and pattern-based network analysis are sufficiently overbroad in their inquiry into protected associations that a person whose associations were investigated or uncovered would have a good claim to standing under *Shelton*.[357] The First Amendment's overbreadth doctrine and the availability of facial challenges to government actions make a lawsuit based on freedom of association rights arguably easier to mount than a Fourth Amendment challenge.[358] Setting aside whether present-day courts would extend *Shelton* to the network analysis context, however, the larger difficulty may be simply finding out what the government is doing with traffic data as long as current minimal statutory thresholds

---

[354] *See* 364 U.S. at 488.
[355] *See* Ellen Nakashima, *A Story of Surveillance*, WASH. POST, Nov. 7, 2007, at D1.
[356] *See Laird*, 408 U.S. at 10.
[357] *See* 364 U.S. at 488.
[358] *See id.*; *Britt*, 574 P.2d at 777.

for obtaining it remain in effect. The public likely will have to rely on whistleblowers and media investigations to obtain basic information about what is being done. Where the relational surveillance to be challenged involves counterterrorism efforts—as it often would—the difficulties of mounting and maintaining a lawsuit in the face of government assertions of state secrets and national security interests are great, as is evident from the course of the recent lawsuits involving the NSA surveillance programs.[359] Civil lawsuits must play an important role in regulating relational surveillance, but more is necessary.

2. The Criminal Context

As Solove pointed out in his article about the general implications of the First Amendment for criminal procedure, one possible mechanism for enforcement of constitutional rights in the surveillance context is an exclusionary rule.[360] The basis for applying an exclusionary rule to evidence obtained in violation of the Fourth Amendment would seem to apply equally well to evidence obtained in violation of the First Amendment's freedom of association protections.[361] Solove suggests that there may be limited power in an exclusionary remedy in the general First Amendment context, because criminal prosecutions are unlikely to occur in many situations in which government information gathering implicates the First Amendment and, even where there are criminal prosecutions, the defendant may not be the one to suffer the First Amendment harm.[362] Although there is some truth to this in the context of relational surveillance as well, there is at least one arena in which an exclusionary rule based on freedom of association might have some teeth—prosecutions under the material support statute.[363]

The material support statute criminalizes the knowing provision of "material support or resources," meaning

> any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communica-

---

[359] *See supra* notes 43–47 and accompanying text.

[360] Solove, *supra* note 9, at 163–64.

[361] *See id.*

[362] *Id.*

[363] *See* 18 U.S.C.A. §§ 2339A–2339B (West 2000 & Supp. 2007). Thanks to Peter Swire for pointing out the connection between relational surveillance and the material support statute.

> tions equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself) and transportation, except medicine or religious materials.[364]

The statute further defines "training," as meaning "instruction or teaching designed to impart a specific skill, as opposed to general knowledge;" and "expert advice or assistance," as meaning "advice or assistance derived from scientific, technical or other specialized knowledge" to those intending to engage in terrorist acts or to certain "designated terrorist organizations."[365] It is notable that the definition of "material support" includes "personnel," which can include the defendant himself or herself if he or she "has knowingly provided, attempted to provide, or conspired to provide a foreign terrorist organization with 1 or more individuals (who may be or include himself) to work under that terrorist organization's direction or control or to organize, manage, supervise, or otherwise direct the operation of that organization."[366]

The material support provision has been controversial in light of its breadth and potential vagueness[367] and some prosecutions under its aegis have been criticized as overreaching.[368] Whatever one thinks of the material support statute itself, it is a context in which the question of the constitutionality of relational surveillance is highly likely to arise because it is at heart a statute that regulates relationships. There are likely to be significant evidentiary issues relating to proof both of the acts required to prove the offense and of the mens rea. If evidence in support of material support prosecutions is obtained using relational surveillance of communications traffic data, there likely will be opportunities to argue that evidence be excluded.

Relying on a freedom of association doctrine developed in the context of an exclusionary rule, however, has disadvantages. First, though the material support statute provides one "hook" into government programs of relational surveillance (and other criminal prosecutions for related crimes of conspiracy and so forth may provide others),

---

[364] *Id.*

[365] *Id.* § 2339A(b)(2)–(3).

[366] *Id.* § 2339A(b)(1); *id.* § 2339B(h).

[367] *See supra* note 11 and accompanying text.

[368] *See, e.g.*, Leslie Eaton, *U.S. Prosecution of Muslim Group Ends in Mistrial*, N.Y. TIMES, Oct. 23, 2007, at A1; Adam Liptak & Leslie Eaton, *Financing Mistrial Adds to U.S. Missteps in Terror Prosecutions*, N.Y. TIMES, Oct. 24, 2007, at A16; Neil MacFarquhar, *Muslim Groups Oppose a List of "Co-Conspirators,"* N.Y. TIMES, Aug. 16, 2007, at A19; Neil MacFarquhar, *U.S., Stymied 21 Years, Drops Bid to Deport 2 Palestinians*, N.Y. TIMES, Nov. 1, 2007, at A18.

not all important issues of relational surveillance will arise in a criminal context.[369] Second, experience with the Fourth Amendment should make one wary about defining rights within the context of an exclusionary rule. The desire to convict the guilty exerts a pressure toward narrow interpretation of the corresponding constitutional rights.

3. The Possibility of Legislative Protection for Freedom of Association

Although legislation is not necessary to mandate protection for freedom of association—the Constitution does that—Congress also bears a responsibility to enforce the Bill of Rights and it has been particularly likely to act in the arena of surveillance regulation.[370] Legislation is particularly helpful in the surveillance context because of the difficulty in detecting constitutional violations ex post and the need for clear direction to law enforcement officials. Legislation can also be used to draw a slightly wider boundary around constitutional rights so as to cabin executive branch discretion.[371] It also provides a clear target for challenges in court when necessary. Given the difficulties in regulating relational surveillance via lawsuits and evidentiary exclusion, Congress should act to protect freedom of association.

There are two ways to regulate relational surveillance by statute. Congress can regulate the circumstances under which law enforcement agents can obtain communications traffic data and under which telecommunications providers can share such data with government agents. Congress can also regulate the uses to which communications data can be put. As a first cut at this issue, it seems reasonable to propose regulations of both types.

a. *Regulation of Sharing of Communications Traffic Data with Law Enforcement*

As discussed in Part III, real time government acquisition of communications traffic data is currently regulated by "pen register" statutes under the Wiretap Act[372] and FISA,[373] which permit law enforcement

---

[369] Solove, *supra* note 9, at 164.

[370] *See* US Const. amend I; *see, e.g.*, Kerr, *Constitutional Myths*, *supra* note 6, at 858 (arguing that Congress is best suited to regulate surveillance using new technologies); Swire, Katz *Is Dead*, *supra* note 6, at 905 (arguing that courts have an important role to play in regulating surveillance using new technologies).

[371] The "super-warrant" provisions of the wiretap act, 18 U.S.C. §§ 2516–2518 (West 2000 & Supp. 2007), and the pen register provision, 18 U.S.C. §§ 3121–3127 (2000 & Supp. IV 2004), play this role, for example.

[372] 18 U.S.C. §§ 3121–3127.

officials to obtain a requisite court order by certifying that the information is "relevant" to "an ongoing criminal investigation" or "an ongoing investigation to protect against international terrorism or clandestine intelligence activities."[374] The FISA provision prohibits the use of a pen register to conduct an investigation of a U. S. person "solely upon the basis of activities protected by the first amendment."[375] Stored electronic communications records may be obtained pursuant to a court order if the records are "relevant and material to an ongoing criminal investigation" or by a NSL if they are "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities," again provided that the investigation is not conducted solely on the basis of activities protected by the First Amendment.[376]

The analysis presented in this Article demonstrates that these hurdles are not sufficient to regulate the use of traffic data for relational surveillance. Given the importance of associational interests involved, at a minimum acquisition of communications traffic data should require a court order. The question remains as to what standard should be applied. It would be possible to impose different standards depending upon whether law enforcement officials intend to apply a network analysis to determine associations. A more workable approach, however, might be to use a reasonable suspicion-type standard[377] to permit the government to intercept communications traffic data or obtain it from stored records only where the information was not only relevant to an ongoing criminal or foreign intelligence investigation, but where there were specific and articulable facts providing reason to believe that the traffic data pertains to an individual guilty of a criminal offense of sufficient seriousness or pertains to a suspected agent of a foreign power.

---

[373] 50 U.S.C.A. § 1842 (West 2003 & Supp. 2007).

[374] 18 U.S.C. § 3122; 50 U.S.C. § 1842.

[375] 50 U.S.C. § 1842(a)(1).

[376] 18 U.S.C.A. § 2709 (West 2000 & Supp. 2007); 50 U.S.C.A. § 1861 (West 2003 & Supp. 2007).

[377] The standard I propose here is similar to that adopted by a recent legislative proposal aimed at regulating NSLs. National Security Letter Reform Act of 2007, S. 2088, 110th Cong. (2007). Though I suggest borrowing some of the language from that legislation, the proposed legislation addresses a somewhat different issue. *See id.* It does not cover obtaining communications traffic data. *See id.* Indeed, the legislation would not permit the use of NSLs to obtain communications traffic data, but only subscriber records. *See id.* Moreover, the legislation deals with NSLs, whereas my proposal would require a court order. *See id.* Note that recent revelations about NSL abuse by the FBI have revived Congressional interest in pursuing NSL reform. Alexei Alexis, *Leahy Says Legislation May Be Needed to Address FBI Data Collection Problems*, Privacy L. Watch (BNA) (Mar. 14, 2008).

In addition to a general provision governing the acquisition of communication traffic data, there should be a specific provision regulating targeted link analysis. A probable cause warrant should be required to instigate a targeted link analysis if it requires the acquisition of communications traffic data beyond that accessible under the general rule already discussed (assuming that the analysis requires the use of traffic data records of individuals who are not reasonably suspected of criminal or terrorist activity). Once such a warrant has been obtained, not only the communications traffic data of the target individual, but also the communications traffic data of individuals for whom there are specific and articulable facts providing reason to believe that they have been in contact with or otherwise directly linked to the target, should be automatically accessible. Obtaining the records of individuals indirectly linked to the target, however, would require an application under the general rule.

Besides these two specific means of obtaining communications traffic data, it might be appropriate to have a third, "catch-all" category in which the First Amendment standard is directly applied by the court considering whether to grant the order.[378] Because a court order would be required (unlike in the NSL situation), the court would be in a position to assess the First Amendment ramifications of any specific circumstances not covered by the two primary provisions.[379] The catch-all provision would permit an order to issue where the court determines that the records pertain to a specific criminal or national security investigation and that obtaining them is a sufficiently narrowly tailored means of pursuing a compelling government interest in light of the potential burdens on expressive and intimate association. It would be wise for Congress to oversee use of such a catchall provision by requiring law enforcement officials to report on their use of it.

b. *Regulation of Pattern-Based Network Analysis*

Besides regulating the acquisition of communications traffic data on a case-by-case basis, Congress should specifically regulate the use of pattern-based network analysis. Congress should begin by banning the use of such analysis to identify criminal or terrorist groups at least

---

[378] This proposal is inspired by a similar provision in the proposed NSL legislation. S. 2088, § 2 (allowing a NSL to issue if obtaining the records is the "least instrusive means" that pertains to activities of a suspected agent of a foreign power).

[379] This is similar to what courts do in assessing subpoenas for association membership information in the context of civil litigation. *See supra* notes 261–275 and accompanying text.

unless and until the accuracy of the algorithms is proven. Congress should also clarify that the standard methods for obtaining communications traffic data may not be used to amass large databases of traffic data for purposes of pattern-based analysis. Congress might wish to authorize research into the possibility of pattern-based analysis and to mandate a report on its technical feasibility and privacy and associational implications. Only if and when congressional investigation demonstrates that pattern-based network analysis is sufficiently accurate to be both useful and protective of civil liberties should any such program be authorized. In this case, usefulness and civil liberties protection are felicitously aligned. Although there are legitimate objections to mere government access to large databases of communications records, the level of harm to freedom of association is closely tied to the extent to which any such algorithm accurately reports only illegitimate activity. The usefulness of any such algorithm similarly depends on its accuracy. Skepticism about whether pattern-based analysis is inherently capable of such distinctions is well warranted. At the least, Congress should require proof of accuracy. If and when such a program is ever authorized, some oversight mechanism must be put into place to vet the specific algorithms to be used and to audit the results.

Conclusion

To summarize, the right to freedom of association under the First Amendment limits government use and acquisition of communications traffic data based on the extent to which the government data use amounts to a disclosure of expressive associations. These limitations are in addition to, and independent of, any limitations arguably deriving from the Fourth Amendment. Moreover, unlike Fourth Amendment protections, which are at least weakened, if not entirely vitiated, by any disclosure to third parties, First Amendment freedom of association rights do not depend on secrecy. Information about association membership in the hands of third parties is still subject to First Amendment protection. Particularly in light of the increasing availability of traffic data and of techniques for analyzing such data to ascertain information about associational structures, current statutory standards are insufficient to meet the requirements of the First Amendment. The First Amendment analysis implicates not only government access to information, but also the technology used to analyze available information.

Broad programs of pattern-based analysis of traffic data, such as may be intended by the alleged NSA acquisition of the call databases

of telephone service providers such as AT&T, are almost certain at this point to be insufficiently aligned with compelling government interests to withstand First Amendment scrutiny because they are likely to expose a large number of legitimate expressive associations (and to fail to identify illegitimate associations). Any programs of pattern-based analysis should be authorized only by specific legislation that provides for hearings into the technical feasibility and accuracy of the proposed approach.

Because of its likelihood to uncover a significant proportion of the target individual's expressive associations, targeted link analysis of a particular individual's associations can comport with First Amendment requirements only when uncovering those associations is closely related to a compelling government interest. A warrant supported by probable cause would be an appropriate prerequisite to such an inquiry. Once such a warrant has been obtained for a link analysis of a target individual's associations, a lesser standard may be appropriate for obtaining traffic data pertaining to other individuals that is necessary to the analysis. This standard should weigh the lesser imposition on the expressive association of such "secondary" individuals against the decreasing potential that the data is pertinent to the focal link analysis the more tenuous the connection to the target individual.

The First Amendment sufficiency of current statutory standards for government obtaining of traffic data is questionable even where there is to be no network analysis. A more stringent standard than mere relevance, which takes into account the right to freedom of association, is needed in some cases, such as those involving the traffic data of an expressive association itself. At a minimum, a court should review requests for traffic data and explicitly consider the potential First Amendment implications raised. When the target of the data gathering is an expressive association, for example, a request for traffic data should meet the probable cause standard discussed above. When the target is an individual and there is no intention to perform link analysis, a materiality standard is the minimum safeguard to ensure that the request is sufficiently related to the government interests at stake. An applicant for such an order should be required to set out facts relevant to the associational issue so that a court can assess whether First Amendment standards are met.

This Article certainly does not pretend to be the last word about how to incorporate freedom of association protections into relational surveillance practices. The freedom of association implications of pattern analysis, in particular, depend on the extent to which the accumulation of the necessary data and the specific algorithmic implementa-

tion are prone to inaccuracy and abuse. How accurately does a particular algorithm distinguish malevolent from protected associative groups? How well does the system protect against abuse by rogue elements or by government itself? Does the system adequately protect against "mission creep" away from truly compelling government interests? Assuming that the system uses some form of anonymizing algorithm, how well does that algorithm protect the anonymity of legitimate associations? How does one balance the possibly greater accuracy obtained by folding more data (including, perhaps, transactional data regarding credit card purchases and so forth) into the analysis with the greater potential chilling effect of a more intrusive government probe into expressive association? Until specific procedures are exposed to scrutiny by the courts under the appropriate First Amendment standard aimed at protecting both mainstream and unpopular expressive activities, these questions cannot be answered with certainty.

We are at an important crossroads for the future of free association. Law enforcement officials charged with preventing terrorism understandably seek to exploit relational analysis for that purpose, leading to pressure to expand the availability of traffic data to government. There are calls for requiring that increasing amounts of traffic data be retained by ISPs and others. It is critical that these calls for increased relational surveillance be balanced by careful analysis both of what is really possible with these new computational technologies and what is at stake for democratic society in light of the increasing importance of technologically mediated emergent association.