

December 2002

Theatrical Investigation: White-Collar Crime, Undercover Operations, and Privacy

Bernard W. Bell

Follow this and additional works at: <https://scholarship.law.wm.edu/wmborj>



Part of the [Criminal Procedure Commons](#)

Repository Citation

Bernard W. Bell, *Theatrical Investigation: White-Collar Crime, Undercover Operations, and Privacy*, 11 Wm. & Mary Bill Rts. J. 151 (2002), <https://scholarship.law.wm.edu/wmborj/vol11/iss1/6>

Copyright c 2002 by the authors. This article is brought to you by the William & Mary Law School Scholarship Repository.

<https://scholarship.law.wm.edu/wmborj>

THEATRICAL INVESTIGATION: WHITE-COLLAR CRIME, UNDERCOVER OPERATIONS, AND PRIVACY

Bernard W. Bell*

The essence of theater is deception. Actors assume various roles to inform or entertain the audience. Frequently, theater takes deception to a second level, in which characters assume false identities or feign loyalty for various purposes. Sometimes such artifices are employed to uncover truths that other seek to keep secret. In *My Fair Lady*, Liza Doolittle assumes the role of an aristocratic lady to test the effect of dialect upon aristocrats' perception of breeding.¹ In *Roman Holiday*, a reporter fails to disclose his occupation to a frustrated young princess in order to discover her innermost desires and chronicle a day in which the princess acts as a commoner.² In *Tootsie*, an actor dresses as a woman to see whether he can fool others into believing that he is.³ *Victor/Victoria* takes such deception to a new level, in which a woman, pretends to be a male entertainer, pretending to be a female entertainer.⁴

Those who seek to ferret out white-collar wrongdoing — criminal investigators, government regulators, journalists, private entities, and individual citizens — emulate such theatrical techniques by using either assumed identities or confidential informants to gather needed information. This article explores the privacy implications of such techniques. I will first briefly outline the use of undercover techniques. I will then suggest that courts use certain modes of privacy to define the scope of individuals' privacy and, often, to enable individuals to define a sphere of privacy for themselves. We will see that the modes of privacy courts most heavily rely upon in defining entitlements against public and private intruders, the modes focusing on physical location and subject matter, do not constrain undercover investigation. Privacy protections can take the form of defining confidential relationships or limiting the means intruders use to discover information. Focusing on such alternative modes of privacy may provide a sounder basis for reconciling the need for undercover techniques with citizens' need for privacy.

I. USE OF UNDERCOVER TECHNIQUES

The use of undercover techniques is ubiquitous. We are most aware of law

* Professor of Law and Herbert Hanoach Scholar, Rutgers School of Law — Newark.

¹ *MY FAIR LADY* (Warner Bros. 1964).

² *ROMAN HOLIDAY* (Paramount Pictures 1953).

³ *TOOTSIE* (Columbia Pictures 1982).

⁴ *VICTOR/VICTORIA* (Metro-Goldwyn Mayer 1982).

enforcement use of such techniques. However, other intruders sometimes rely upon undercover techniques.

A. Government

The government uses undercover techniques in at least two capacities: criminal and regulatory. In the context of the Fourth and Fifth Amendments, the Supreme Court has distinguished criminal investigation from administrative regulation.⁵ Thus, for example, the government possesses much greater authority to conduct warrantless searches attendant administrative enforcement of Occupational Health and Safety regulations or management of the country's borders than it does when investigating routine criminal violations.⁶ Similarly, courts have interpreted the Fifth Amendment to allow government-mandated record-keeping in regulatory contexts that might otherwise violate the Fifth Amendment if imposed to facilitate investigation of routine criminal conduct.⁷ Thus, it is helpful to consider the use of undercover operations in criminal investigation and in regulatory enforcement separately.

1. Criminal Investigation

Use of undercover techniques to reveal crimes, particularly white-collar crimes, is common, though not well-documented.⁸ One noted scholar, Gary Marx, has

⁵ See *United States v. Brignoni-Ponce*, 422 U.S. 873, 883 n.8 (1975) (finding that searches for immigration purposes do not violate the Fourth Amendment); *Almeida-Sanchez v. United States*, 413 U.S. 266, 272-75 (1973); cf. *Delaware v. Prouse*, 440 U.S. 648, 665 (1979) (Rehnquist, J., dissenting) (arguing that random automobile stops without suspicion violate the Fourth Amendment when conducted for criminal investigation purposes); see also *Ferguson v. City of Charleston*, 532 U.S. 67, 79-81 (2001) (addressing testing for illegal narcotics during routine medical procedures); *City of Indianapolis v. Edmund*, 531 U.S. 32, 38-42 (2000) (addressing the use of drug interdiction checkpoints).

⁶ *Marshall v. Barlow's, Inc.*, 436 U.S. 305, 320 (1978) (addressing workplace searches conducted by OSHA inspectors to enforce workplace safety regulations); *Brignoni-Ponce*, 422 U.S. at 883 n.8 (addressing interdiction of vehicles in areas near the nation's borders by INS agents); *Almeida-Sanchez*, 413 U.S. at 272-75 (addressing search of automobile in area near the nation's borders by INS agents).

⁷ See *Selective Serv. Sys. v. Minn. Pub. Interest Research Group*, 468 U.S. 841 (1984); *Shapiro v. United States*, 335 U.S. 1 (1948); William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1017-18 (1995). William Stuntz discusses the dilemmas brought about by the dichotomy between criminal investigation and regulation, noting that the rule in *Boyd v. United States*, 116 U.S. 616 (1886), seemed to balance the individual's interests in privacy and the state's interest in the context of criminal investigation, but threatened to nullify the government's power to regulate commercial activity. *Id.* at 1029-34.

⁸ See, e.g., Edward M. Neafsey, *Why a Division of Criminal Justice?*, 25 SETON HALL

argued that deceptive investigative techniques have displaced the coercive means of investigation.⁹ He has noted that constitutional doctrine developed since the 1960s has largely limited coercive investigative techniques such as searches or intimidating methods of interrogation. Use of undercover techniques for

LEGIS. J. 107, 124–33 (2001) (discussing the undercover investigation of environmental criminals); see also *Cross-Border Fraud: Hearing Before the Subcomm. on Investigations, Senate Comm. on Governmental Affairs*, 107th Cong. 162–63 (2001) (prepared statement of Mary Ellen Warlow, Acting Deputy Assistant Attorney General, U.S. Department of Justice) (discussing undercover operations directed at telemarketing fraud); *Investigative Practices of Inspectors General: Hearing Before the Subcomm. on Gov't Mgmt., Info., & Tech., House Comm. on Gov't Reform*, 105th Cong. (June 24, 1997) (statement of Eleanor Hill, Inspector General, U.S. Department of Defense) (discussing the use of undercover techniques to investigate procurement and contracting fraud and other white-collar crimes), 1997 WL 345159. See generally GARY T. MARX, UNDERCOVER: POLICE SURVEILLANCE IN AMERICA 37–40 (1988) (discussing the use of undercover techniques to investigate white-collar crime).

A computerized search of the *Andrews White-Collar Crime Reporter* reveals a number of cases resulting from undercover operations. E.g., *Banker Pleads Guilty to Money Laundering*, 15 White-Collar Crime Rep. (Andrews Publ'n) No. 9, at 11 (Oct. 2001) (describing the arrest of investment banker who agreed to launder money for an undercover agent posing as an arms trader); *DOT Employee Charged with Bribery*, 15 White-Collar Crime Rep. (Andrews Publ'n) No. 9, at 11 (Oct. 2001) (describing operation in which an employee of the Maritime Administration accepted a bribe of NASCAR tickets from an undercover agent posing as a contractor); *Feds Charge Defense contractor With Mail Fraud*, 16 White-Collar Crime Rep. (Andrews Publ'n) No. 2, at 7 (Feb. 2002) (discussing the undercover investigation of a defense contractor for sale of uninspected and defective parts for use in military planes); *Feds Execute 100 Search Warrants in Software Copyright Probe*, 16 White-Collar Crime Rep. (Andrews Publ'n) No. 1, at 1 (Jan. 2002) (describing Operation Bandwidth, a sting operation in which software pirates provided undercover agents with "over 100,000 computer files and 12,000 stolen software programs"); *Indictment Stands for E-Mailing Document Across State Lines*, 15 White-Collar Crime Rep. (Andrews Publ'n) No. 6, at 13 (July 2001) (describing operation in which a paralegal attempted to sell a trial plan to an FBI agent posing as opposing counsel); *Jury Convicts Diet Drug Doc on 14 Counts of Selling Drugs Illegally*, 13 White-Collar Crime Rep. (Andrews Publ'n) No. 5, at 12 (describing an undercover DEA investigation of a doctor prescribing weight-loss drugs to patients who did not need them); *Money Laundering Investigation Results in Guilty Plea*, 16 White-Collar Crime Rep. (Andrews Publ'n) No. 6, at 15 (June 2002) (describing undercover IRS investigation); *Organized Crime Implicated in Securities Fraud Arrests*, 15 White-Collar Crime Rep. (Andrews Publ'n) No. 7, at 17 (describing a year-long undercover operation by the FBI, in cooperation with SEC and NASD); *TN Man Convicted of Selling Illegal Gaming Devices, Laundering Money*, 13 White-Collar Crime Rep. (Andrews Publ'n) No. 4, at 17 (describing a state undercover investigation of a company illegally manufacturing and distributing video poker and slot machines); *Va. Man Sentence for Selling Fake Asbestos Training Certificates*, 14 White-Collar Crime Rep. (Andrews Publ'n) No. 5, at 7 (describing an undercover EPA investigation).

⁹ MARX, *supra* note 8, at 47.

conventional investigative purposes became particularly controversial as a result of the FBI's ABSCAM investigation and with the use of undercover techniques in white-collar investigations more generally.¹⁰ Such techniques once again became controversial as a result of Special Prosecutor Kenneth W. Starr's investigation of President Bill Clinton, who used tapes Linda Tripp made of conversations with Monica Lewinsky, encouraged Tripp to make additional recordings, and even considered having Monica Lewinsky surreptitiously record her conversations with President Clinton.¹¹

Law enforcement officials continue to rely heavily on undercover techniques in narcotics investigations. Such techniques, however, are arguably also essential in investigating certain white-collar offenses. White-collar crime may be virtually impossible to uncover by nondeceptive means because many white-collar offenses involve deception and abuse of legitimate authority.¹² In contrast, many traditional crimes involve use of force, rather than deception.

2. Regulators

Regulatory agencies sometimes use undercover techniques for purposes of assuring that regulated entities comply with legal requirements.¹³ The goal may not

¹⁰ *Id.* at 8–10.

¹¹ Bernard W. Bell, *Secrets and Lies: News Media and Law Enforcement Use of Deception as an Investigative Tool*, 60 U. PITT. L. REV. 745, 810 n.295 (1999); Angela J. Davis, *The American Prosecutor: Independence, Power, and the Threat of Tyranny*, 86 IOWA L. REV. 393, 417 & nn. 103–04 (2001); Judy Keen & Kevin Johnson, *Tripp Testifies for a 4th Day*, USA TODAY, July 10, 1998, at 11A (citing poll showing that most Americans were against making tapes); Kathleen Parker, *What Are Friends For? Why Did Tripp Tape Conversations with Intern?*, PEORIA J. STAR, Jan. 26, 1998 at A4 (editorializing that taping conversations was as bad as an adulterous affair); see also Gary Fields, *Privacy Watchers Criticize Starr, Say Tactics Will Have Repercussions For Others*, USA TODAY, Apr. 16, 1998, at 6A (noting that Starr's aggressive investigative tactics put the privacy issue in the spotlight); Ruth Marcus, *To Some in the Law Starr's Tactics Show a Lack of Restraint*, WASH. POST, Feb. 13, 1998, at A1 (questioning whether Starr's investigation was too aggressive).

¹² See Peter J. Henning, *Testing the Limits of Investigating and Prosecuting White Collar Crime: How Far Will the Courts Allow Prosecutors to Go?*, 54 U. PITT. L. REV. 405, 406 (1993) ("White collar crime . . . involves a process of events, many of which are common business occurrences that may be otherwise socially desirable. The white collar criminal's goal is to conceal all evidence that a crime has been committed while preserving the patina of legality surrounding the normal conduct of business.").

¹³ See *Bradley v. Med. Bd.*, 65 Cal. Rptr. 2d 483, 491 & n.13 (Cal. Ct. App. 1997) ("As attested to by a supervising investigator for the Board, '[u]ndercover operations are routinely used by the Medical Board . . . to investigate complaints . . . of overprescribing or drug addiction'); OHIO ADMINISTRATIVE LAW HANDBOOK AND AGENCY DIRECTORY § 3.11 (West, WESTLAW through June 2002) (discussing the use of undercover investigations by

be criminal prosecution (though that is a possibility)¹⁴ but rather disqualifying the unqualified, preventing further violations, or perhaps compensating victims.¹⁵ However, regulatory agencies possess much broader powers than criminal investigators to conduct searches and coerce disclosure of incriminating information. Moreover, the administrative search doctrine allows regulators (unlike law enforcement officials) to conduct routine inspections of premises without probable cause to believe a regulatory violation exists, much less that a crime has been committed.¹⁶ The Fourth Amendment, as construed by the United States Supreme Court, also allows for warrantless searches in pervasively regulated industries.¹⁷

The Fifth Amendment ordinarily constrains criminal investigators efforts to obtain incriminating statements from suspected wrongdoers. However, the Fifth Amendment privilege against self-incrimination often does not hamper regulators' use of compulsory process to secure information regarding a regulatory violation. Indeed, the federal government requires enormous amounts of record keeping for a variety of purposes, including assessing the need for regulation and ensuring regulated entities' compliance with legal obligations.¹⁸ Commercial enterprises in

state agencies); 22 TEX. ADMIN. CODE § 75.4 (West, WESTLAW through 2002 legislation) (setting forth the rules governing undercover investigations of chiropractic examinations).

¹⁴ E.g., *New York v. Burger*, 482 U.S. 691 (1987); *Whalen v. Roe*, 429 U.S. 589 (1977).

¹⁵ *Bradley*, 65 Cal. Rptr. 2d at 483; MARX, *supra* note 8, at 86–88.

In late 1997, the Equal Employment Opportunity Commission announced that it would use undercover techniques to investigate employment discrimination. See Katherine Q. Seelye, *Agents to Go Undercover in Detection of Hiring Bias*, N.Y. TIMES, Dec. 7, 1997, § 1, at 31.

¹⁶ *Marshall v. Barlow's, Inc.*, 436 U.S. 307, 321 (1978) (finding a search to be constitutional if an agency obtains a warrant based not on individualized suspicion, but rather on a "showing that a specific business has been chosen for an OSHA search on the basis of a general administrative plan for the enforcement of the Act derived from neutral sources"); See *v. Seattle*, 387 U.S. 541 (1967) (holding a warrant necessary for a fire inspection, but that the warrant need not be based on individualized suspicion).

¹⁷ *Burger*, 482 U.S. at 691 (inspection of automobile junkyard); *Donovan v. Dewey*, 452 U.S. 594 (1981) (mine inspections); *United States v. Biswell*, 406 U.S. 311 (1972) (warrantless search of firearm dealer's business premises); *Colonnade Catering Corp. v. United States*, 397 U.S. 72 (1970) (inspection of liquor retailer's premises); See *v. City of Seattle*, 387 U.S. 541, 546 (1967) ("[N]or do we question such accepted regulatory techniques as licensing programs which require inspections prior to operating a business or marketing a product.").

¹⁸ OFFICE OF INFO. & REGULATORY AFFAIRS, OFFICE OF MGMT. & BUDGET, MANAGING INFORMATION COLLECTION AND DISSEMINATION, at 8, 21 (2002), available at http://www.whitehouse.gov/omb/infoereg/paperwork_policy_report_final.pdf; see also *Byers v. California*, 402 U.S. 424, 427–28 (1971).

Such requirements would violate the Fifth Amendment if directed toward uncovering conventional crimes rather than regulatory transgressions or regulated activity. *Marchetti v. United States*, 390 U.S. 39 (1968) (overturning conviction for failure to register and pay

pervasively regulated industries may be required to comply with subpoenas and maintain records as a part of their permission to do business.¹⁹

Moreover, the Fifth Amendment privilege against self-incrimination will not likely prohibit the use of compulsory process to secure information indicating a regulatory violation for a second reason. Entities engaged in commercial activities will often be legally distinct from the particular individual whom its records may incriminate. While individuals may interpose Fifth Amendment objections to compulsory process seeking incriminating testimony from themselves, they generally may not raise such objections when compulsory process requires a legally distinct entities to produce incriminating records held by it.²⁰

All this might suggest less of a need for undercover operations in the regulatory context because regulators possess more efficacious investigative powers.²¹ Nevertheless, regulators do use undercover techniques. Indeed, sometimes regulators and criminal investigators work together, blurring the line between regulation and criminal investigation.²²

federal wagering tax); *Albertson v. Subversive Activities Control Bd.*, 382 U.S. 70 (1965) (overturning order requiring Communist Party members to register or face criminal penalty); *see also* *Leary v. United States*, 395 U.S. 6 (1969); *Haynes v. United States*, 390 U.S. 85 (1968); *Grosso v. United States*, 390 U.S. 62 (1968); John H. Mansfield, *The Albertson Case: Conflict Between the Privilege Against Self-Incrimination and the Government's Need for Information*, 1966 SUP. CT. REV. 103; Robert B. McKay, *Self Incrimination and the New Privacy*, 1967 SUP. CT. REV. (1967).

¹⁹ *Cal. Banker's Ass'n v. Shultz*, 416 U.S. 21 (1974) (banking industry); *United States v. Morton Salt Co.*, 338 U.S. 632, 636–37 (1950) (Federal Trade Commission subpoena); *see also* *Shapiro v. United States*, 335 U.S. 1, 18–19 (1948) (subpoena issued under authority of the Emergency Price Control Act); *Wilson v. United States* 221 U.S. 361, 380 (1911) (holding that custodian cannot raise Fifth Amendment claim to subpoena for “records required by law to be kept in order that there may be suitable information of transactions which are the appropriate subjects of governmental regulation, and the enforcement of restrictions validly established”); KENNETH CULP DAVIS & RICHARD J. PIERCE, JR., *ADMINISTRATIVE LAW TREATISE* § 4.11, at 178–80 (3d ed. 1994); Peter J. Henning, *Testing the Limits of Investigating and Prosecuting White Collar Crime: How Far Will the Courts Allow Prosecutors to Go?*, 54 U. PITT. L. REV. 405, 439–41 (1993). *See generally* RICHARD J. PIERCE, JR. ET AL., *ADMINISTRATIVE LAW AND PROCESS* § 8.1, at 399 n.4 (3d ed. 1999) (outlining extensive licensing regimes that impose compelled report filing requirements on licensees).

²⁰ WAYNE R. LAFAYE ET AL., *CRIMINAL PROCEDURE* § 8.12(b) (3d ed. 2000); *see also* *Doe v. United States*, 487 U.S. 201 (1988); *Braswell v. United States*, 487 U.S. 99 (1988); *United States v. Doe*, 465 U.S. 605 (1984); *Fisher v. United States*, 425 U.S. 391 (1976); Peter J. Henning, *Testing the Limits of Investigating and Prosecuting White Collar Crime: How Far Will the Courts Allow Prosecutors to Go?*, 54 U. PITT. L. REV. 405, 415–39 (1993).

²¹ MARX, *supra* note 8, at 47 (“[R]estrict police use of coercion, and the use of deception increases. Restrict investigative behavior after an offense, and increased attention will be paid to anticipating an offense.”).

²² Michael L. Benson, *Investigating Corporate Crime: Local Responses to Fraud and*

B. Journalists

Journalists have also long engaged in undercover investigation.²³ Two renowned early undercover investigations involved Nellie Bly and Upton Sinclair. Bly investigated the conditions at a New York City mental institution in the 1880s. She did so by checking into a boarding house and acting strangely, prompting police officers to take her to the mental institution for commitment. Bly acted normally thereafter, but authorities at the institution continued to confine her. After ten days Bly's editor secured her release. Bly wrote a first person account of her incarceration.²⁴ Upton Sinclair posed as a meatpacker to investigate the conditions in slaughterhouses, and afterward wrote a highly acclaimed book-length expose.²⁵

The rise of investigative reporting and broadcast journalism has spurred greater use of undercover techniques. Broadcast journalism encourages use of undercover techniques because it places greater demands on journalists for dramatic visual images. Litigation arising out of ABC's use of undercover techniques to investigate meat handling practices at a supermarket chain has sparked debate about journalistic use of undercover techniques.²⁶

ABC's *PrimeTime Live* decided to investigate conditions at Food Lion supermarkets, after receiving allegations that the chain engaged in unsanitary practices. Two *PrimeTime Live* producers, Lynn Litt and Susan Barnett applied for jobs as meat packers in two separate Food Lion stores, using false identities and providing falsified references. Once hired, Litt and Barnett observed various unsanitary practices and recorded the unsanitary conditions and practices with hidden cameras and tape recorders. Litt and Barnett recorded about forty-five hours of material while working as Food Lion employees. ABC televised a story on conditions at Food Lion featuring Litt and Barnett's surreptitiously made film and audio tape.

Food Lion brought suit claiming breach of duty of loyalty, trespass, fraud, and unfair trade practices. Food Lion proffered two breach of loyalty theories. First, the two *PrimeTime Live* producers had breached their duty of loyalty as Food Lion employees by providing information to ABC. Second, Litt and Barnett had breached their duty of loyalty to Food Lion by performing their duties at Food Lion less proficiently than they would have had they not been trying to gather damaging

Environmental Offenses, 28 W. ST. U. L. REV. 87, 89 (2000–2001).

²³ Lyrisssa Barnett Lidsky, *Prying, Spying, and Lying: Intrusive Newsgathering and What the Law Should Do About It?*, 73 TUL. L. REV. 173, 231–32 (1998); David A. Logan, "Stunt Journalism," *Professional Norms, and Public Mistrust of the Media*, 9 U. FLA. J.L. & PUB. POL'Y 151, 151–57 (2002).

²⁴ This was not Bly's only undercover investigation. BROOKE KROEGER, NELLIE BLY: DAREDEVIL, REPORTER, FEMINIST 87–88 (1994); Logan, *supra* note 23, at 152–53.

²⁵ UPTON SINCLAIR, *THE JUNGLE* (Heritage Press 1965) (1906).

²⁶ Food Lion, Inc. v. Capital Cities/ABC, Inc., 194 F.3d 505 (4th Cir. 1999).

information for a news story. The trespass claim was grounded on Litt and Barnett's entry of non-public areas of Food Lion's facilities under false pretenses. Food Lion's fraud claim alleged that the company had spent money hiring and paying the two *Primetime Live* producers based upon their misrepresentations. The unfair trade practices claim was based on the North Carolina Uniform Trade Practices Act, which prohibits "unfair methods of competition" and "unfair or deceptive acts or practices." Food Lion alleged that Litt's misrepresentations on her job application constituted prohibited "deceptive acts."

The jury awarded substantial damages, largely consisting of punitive damages. The trial court reduced the damage award, but upheld the liability determination. The court rejected the claim that Litt and Barnett had breached their duty of loyalty by providing information to ABC, concluding that the information the two had divulged was not the type of information protected by the breach of loyalty cause of action. The court held that the second breach of loyalty claim (focused on Litt and Barnett's failure to concentrate exclusively on their responsibilities at Food Lion) stated a valid cause of action, but only a small portion of the damages award was attributable to that breach of loyalty.

The Fourth Circuit upheld two aspects of the claim: breach of duty of loyalty (based on Litt and Barnett's divided loyalties) and trespass, but noted that each had resulted in merely nominal damages. It dismissed the unfair trade practices claim because the deception ABC and its producers had engaged in was not generally actionable under North Carolina law.²⁷

Journalists' goals in conducting undercover investigations differ from those of both law enforcement officials and regulators. Journalists have little interest in collecting evidence for criminal prosecution. Indeed, their interests are not limited to uncovering illegal activity.²⁸ Journalists' really seek exposure, whether the matters exposed consist of unlawful activity or other activity of interest to their audience.

Such exposure enables public discussion of certain practices and allows democratic bodies to decide whether additional regulation or some other response is appropriate.²⁹ Such efforts also provide a more personal, individual benefit to readers and viewers, in particular, allowing them to exercise autonomy. Some media undercover investigations allow readers and viewers to learn about the true qualities of the persons or entities with which they interact rather than the facade

²⁷ *Id.* The case has spawned numerous law review articles and popular commentaries.

²⁸ *Sanders v. Am. Broad. Co.*, 978 P.2d 67 (Cal. 1999) (hidden-camera examination of the work of telephone psychics); Howard Kurtz, *Gifford Tumbles into Tabloid Trap: Globe's Tactics in Liason Cause a Stir*, WASH. POST, May 17, 1997, at H1 (investigation of celebrity Frank Gifford's marital fidelity to his television personality spouse Kathie Lee Gifford)).

²⁹ The prime example is the enactment of the Pure Food and Drugs Act, Pub. L. No. 59-384, 34 Stat. 768 (1906), after Upton Sinclair's undercover exposé of the meat-packing industry. See SINCLAIR, *supra* note 25.

they maintain. Thus, journalists' justification for employing undercover methods resembles those offered by law enforcement. Specifically, journalists cannot otherwise obtain some information because those who engage in illegal or improper conduct, particularly white-collar miscreants, will deceive known outsiders.³⁰

While some undercover investigations pursued by journalists have been elaborate,³¹ almost all are much simpler than the more ambitious law enforcement undercover investigations. The expense, danger, and potential need to violate the law sometimes required by effective undercover operations (and the wiretap laws' more stringent limitations on journalists) restrict journalists to a greater degree than law enforcement officials.³² Journalists, however, may conduct such investigations independently or in conjunction with law enforcement or regulators.

C. Other Private Citizens

People who are neither journalists nor government officials employ undercover techniques in a variety of contexts. For example, fair housing organizations use testers to determine whether realtors treat minority and non-minority clients equally.³³ Employers may use decoys to test the integrity, or even the courtesy, of their employees.³⁴ So far, such private "stings" have not become as controversial as law enforcement "stings" or journalist hidden-camera investigations.

II. THE LAW OF PRIVACY

The protection provided by the law of privacy differs depending on whether the source of the potential intrusion is a governmental or nongovernmental entity. Government intrusion into privacy is constrained by the Fourth Amendment of the United States Constitution, limiting government searches and seizures.³⁵ Fourth

³⁰ Diane Leenheer Zimmerman, *I Spy: The Newsgatherer Undercover*, 33 U. RICH. L. REV. 1185, 1206 (2000); see also Lori Keeton, Note, *What Is Really Rotten in the Food Lion Case: Chilling the Media's Unethical Newsgathering Techniques*, 49 FLA. L. REV. 111 (1997); *ABC PrimeTime Live: Hidden Camera, Hard Choices* (ABC television broadcast, Feb. 12, 1997) (discussing the *Food Lion* case with jurors).

³¹ For example, the *Chicago Sun-Times* purchased and operated a bar to document corruption among various inspectors employed by the City of Chicago. See ZAY N. SMITH & PAMELA ZEKMAN, *THE MIRAGE* (1979); Zay N. Smith & Pamela Zekman, *The Mirage Takes Shape*, 18 COLUM. JOURNALISM REV. 51 (1979).

³² See Bell, *supra* note 11, at 778-79. For instance, presumably no news organization would have conducted an operation like ABSCAM, in which informants offered bribes to members of Congress, or Operation Greylord, involving investigation of judicial bribery.

³³ See Bell, *supra* note 11, at 835.

³⁴ Peter Scott, *Indifferent Clerks, Surly Cashiers. What Is to Be Done?*, WALL ST. J., June 29, 2001, at W17 (discussing the \$435 million "secret shopper" industry).

³⁵ U.S. CONST. amend. IV; LAFAYETTE ET AL., *supra* note 20, §§ 3.1-10; Bell, *supra* note

Amendment analysis involves a two-step process. First, a court must determine whether law enforcement officers have breached any reasonable expectation of privacy — in other words, the court must determine whether the investigative target has any cognizable privacy interest at all.³⁶ If the court concludes that the target did possess a legitimate expectation of privacy, the court must then decide whether the Fourth Amendment permits the breach of that privacy expectation — because either the police have secured a warrant after establishing probable cause, or the breach fits within one of numerous judicially recognized exceptions to the warrant and probable cause requirements.³⁷

The Fifth Amendment protections against self-incrimination may also protect privacy in certain circumstances.³⁸ The substantive criminal law doctrine of entrapment, absolving defendants when law enforcement officials have involved themselves too substantially in the criminal activity for which they seek to prosecute the defendant, can also protect privacy in certain circumstances.³⁹ In addition, given the limited nature of constitutional protections of privacy against government intrusions, Congress has enacted federal statutes that supplement Fourth Amendment protections of privacy — statutes that, for example, limit government wiretapping or government access to bank records.⁴⁰ Other statutes limit government disclosure of private information in government databases without consent.⁴¹ As

11, at 755–56.

³⁶ *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

³⁷ *Id.* at 357.

³⁸ Robert Gerstein, *Privacy and Self-Incrimination*, in *PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY* 245 (Ferdinand David Schoeman ed., 1984).

³⁹ Some prosecutions based on particularly troublesome undercover operations have foundered on entrapment or related constitutional defenses. *See, e.g., State v. Lively*, 921 P.2d 1035, 1046, 1048–49 (Wash. 1996) (dismissing prosecution against narcotics addict who sold drugs to a confidential informant, explaining that the police had deprived the criminal defendant of due process by, *inter alia*, authorizing a confidential informant to attend narcotics anonymous meetings to lure recovering drug addicts to engaged in illegal drug transactions). Ultimately, however, entrapment law focuses on the defendant's predisposition to commit a crime, not the legitimacy of police deception. *See United States v. Russell*, 411 U.S. 423, 435–36 (1973) (stating that the entrapment defense was not intended to allow the federal judiciary to punish “overzealous law enforcement,” or exercise a “chancellor’s foot” veto over law enforcement practices of which it did not approve,” but rather the entrapment defense rests on the principle that Congress could not have intended criminal punishment for a defendant who was induced by the government to commit an offense). *See generally* LAFAYE ET AL., *supra* note 20, §§ 5.1–.2; WAYNE R. LAFAYE & AUSTIN W. SCOTT, JR., *CRIMINAL LAW* § 5.2 (2d ed. 1986); MARX, *supra* note 8, at 188–90.

⁴⁰ Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3697 (codified as amended at 12 U.S.C. §§ 3401–3422) (2000); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 301, 100 Stat. 1848, 1868–72 (codified as amended at 18 U.S.C. §§ 3121–3127 (2000)).

⁴¹ Privacy Act of 1974, Pub. L. No. 93-579 (codified at 5 U.S.C. § 552a) (covering

noted above, judicially developed constitutional doctrines distinguish regulation and criminal investigation so as to afford regulators enhanced powers to obtain information from private citizens.⁴²

The protection of privacy against nongovernmental intruders, whether journalists or other private citizens, rests upon an amalgam of statutory and common law. Private actors, unlike governmental actors, are not subject to constitutional constraints—thus the Fourth and Fifth Amendments generally do not limit their intrusions.⁴³ A cluster of common-law causes of action directly protect various aspects of privacy. In particular, courts have recognized four “privacy” causes of action: intrusion into seclusion, disclosure of private facts, false-light privacy, and appropriation of likeness.⁴⁴ Generally, a person commits the tort of intrusion if: (1) he “intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns,” and (2) the intrusion “would be highly offensive to a reasonable person.”⁴⁵ Secretly planting a listening device in a married couple’s bedroom provides the classic example of such intrusive behavior. The intrusion cause of action focuses on the means with which the defendant obtained the information, and indeed the plaintiff need not even prove dissemination of any information discovered as a result of the intrusion.⁴⁶ By contrast, the other privacy causes of action turn on the disclosure of information or images rather than their acquisition.

The disclosure of private facts cause of action allows individuals to recover compensation when others publicize their private matters. To prevail on such a claim, plaintiff must show that the defendant gave publicity to an aspect of plaintiff’s private life, that such publicity would be “highly offensive to a reasonable person,” and that the publicized information “is not of legitimate concern to the public.”⁴⁷

records maintained by federal agencies); Driver’s Privacy Protection Act of 1994, Pub. L. No. 103-322, 108 Stat. 2099 (codified at 18 U.S.C. §§ 2721–2725) (covering records maintained by state motor vehicle agencies).

⁴² See *supra* notes 8–19 and accompanying text.

⁴³ *Burdeau v. McDowell*, 256 U.S. 465, 475–77 (1921) (holding that the Fourth Amendment protects against unreasonable searches and seizures by the government and was not intended as a limitation upon nongovernmental entities); *State v. von Bulow*, 475 A.2d 995, 1012 (R.I. 1984) (“[T]he constitutional prohibition of unreasonable searches and seizures applies only to governmental conduct.”) (quoting *State v. Eiseman*, 461 A.2d 369, 374 (1983)); *LAFAVE ET AL.*, *supra* note 20, § 3.1(h).

⁴⁴ See William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960) (creating these categories); see also RESTATEMENT (SECOND) OF TORTS § 652A (1977) (adopting this categorization).

⁴⁵ RESTATEMENT (SECOND) OF TORTS § 652B.

⁴⁶ *Hamberger v. Eastman*, 106 N.H. 107, 111–12, 206 A.2d 239 (1964); RESTATEMENT (SECOND) OF TORTS § 652B cmt. a.

⁴⁷ RESTATEMENT (SECOND) OF TORTS § 658D.

The false light privacy cause of action supplements defamation liability and arguably does little to protect privacy. False light privacy focus on false statements about a person that do not harm reputation but convey a misimpression about the individual's personality and attributes.⁴⁸ Thus, to make out a claim for false light privacy, the plaintiff must establish that the defendant has given publicity to the plaintiff in a way that puts him before the public in a false light, that such false light would be highly offensive to the reasonable person, and that the defendant acted with knowledge or reckless disregard with respect to the falsity of the publicized matter. One prominent false light privacy claim involved the use of a photograph depicting a child killed by a car to illustrate a story about pedestrian carelessness, even though the child's injury had not been due to her negligence.⁴⁹

Finally, the appropriation of name or likeness cause of action seeks to vindicate a person's interest in avoiding nonconsensual commercial exploitation of her identity.⁵⁰ The classic example of a situation covered by the tort is one in which a company uses a photograph of a person's face or their name to advertise a product.⁵¹

States vary in the common-law privacy causes of action they recognize.⁵² For example, New York recognizes only the privacy cause of action for appropriation of likeness.⁵³

Other common-law causes of action can vindicate individuals' interests in privacy, even though the causes of action themselves are not focused on protecting privacy. Some plaintiffs have asserted common-law trespass and breach of confidence causes of action against intrusion.⁵⁴ Invoking real property rights to

⁴⁸ *Id.* § 652D cmt. b.

⁴⁹ *Leverson v. Curtis Publ'g Co.*, 192 F.2d 974 (3d Cir. 1951).

⁵⁰ RESTATEMENT (SECOND) OF TORTS § 658C.

⁵¹ *Robertson v. Rochester Folding Box Co.*, 64 N.E. 442 (N.Y. 1902) (addressing use of an infant girl's photograph with the caption "Flour of the Family" in advertisement for defendant's flour); *Pavesich v. New England Life Ins. Co.*, 50 S.E. 68 (Ga. 1905) (addressing use of plaintiff's photograph and name in newspaper advertisement for defendant's insurance company). Though the New York Court of Appeals refused to recognize a common-law cause of action in *Robertson*, the New York legislature created a statutory cause of action in response to the decision. 1903 N.Y. Laws ch. 132, §§ 1, 2 (codified at N.Y. CIV. RIGHTS LAW §§ 50, 51 (1984)).

⁵² See generally 1 ROBERT D. SACK, SACK ON DEFAMATION: LIBEL, SLANDER, AND RELATED PROBLEMS § 12.2.2 (3d ed. 2002); 62A AM. JUR. 2D *Privacy* §§ 5-7 (1990).

⁵³ N.Y. CIV. RIGHTS LAW §§ 50-51 (1984); 62A AM. JUR. 2D § 12; see also *supra* note 49.

⁵⁴ See Bell, *supra* note 11:

At common law, employees owed their employer a duty of loyalty. That duty of loyalty included an obligation to keep confidential the employer's valuable trade secrets. Thus, employers have long possessed a right to compensation for any damage resulting from an employees' disclosure of trade secrets.

Id. at 759 (citations omitted).

exclude strangers from one's property can effectively secure one's privacy while one remains secluded on his or her property.⁵⁵ Similarly, to the extent that an intruder becoming an employee of the target company, a breach of confidence cause of action might be invoked to prevent disclosure of information the intruder obtains as a result. While the cause of action is focused on protecting economic interests, namely trade secrets, it could potentially be invoked to protect the firm's "privacy" interest.⁵⁶

The federal and state governments have also enacted statutes protecting various aspects of privacy.⁵⁷ For example, federal statutes prohibit private individuals from surreptitiously intercepting conversations. Federal statutes also require entities to keep banking account information, video rental records, and educational records confidential. Statutes also place limitations on the dissemination of consumer credit information.⁵⁸ Recently promulgated Department of Health and Human Services regulations require medical personnel to keep patient records confidential.⁵⁹

III. THE MODES OF PRIVACY PROTECTION

Defining the contours of individuals' legitimate expectations of privacy in personal information presents courts and legislatures with a daunting task. In other words, specifying the types of information concerning individuals that should be designated "private," and thus immune from snooping and discussion by others, entails great difficulties. Whether such information should be recognized as "private" surely depends heavily on the circumstances — an individual's HIV-positive status may properly be deemed "private" vis-a-vis employers, neighbors,

⁵⁵ See generally RESTATEMENT (SECOND) OF TORTS § 158 (1965); W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 13, at 67–84 (5th ed. 1984).

⁵⁶ Evidentiary privileges also may play a role in protecting privacy. See *infra* notes 181–94 and accompanying text.

⁵⁷ See, e.g., Video Privacy Protection Act of 1988, Pub. L. No. 10-618, 102 Stat. 3195 (codified at 18 U.S.C. § 2710) (preventing video rental outlets from disclosing rental and sales information); Employee Polygraph Protection Act of 1988, Pub. L. No. 100-347, 102 Stat. 646 (codified at 29 U.S.C. § 2001) (limiting employers' ability to subject employees and job applicants to polygraph tests); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. § 2510) (regulating the conditions under which interception of wire and oral communications may be authorized); Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 88 Stat. 571 (codified at 20 U.S.C. § 1232g) (restricting educational institutions ability to disclose educational and related information of students and their parents); Confidentiality of HIV-Related Information Act, 1990 Pa. Laws 584-148 (codified at 35 PA. CONS. STAT. §§ 7601–7612 (2002)).

⁵⁸ Fair Credit Reporting Act, Pub. L. No. 90-321, 84 Stat. 1128 (1968) (codified as amended at 15 U.S.C. §§ 1681–1681t) (regulating the information creditors may disclose).

⁵⁹ E.g., Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (to be codified at 45 C.F.R. pts. 160, 164).

and the general public, but not vis-a-vis past, present, and future sexual partners.

Moreover, individuals have vastly different privacy preferences, and the information or activities they wish to keep private may vary greatly. Some may have little desire to keep their sexual practices or their bodies private while others may care little about maintaining the confidentiality of their financial circumstances. Given the difficulty in setting forth facts or activities that should be designated "private," legislatures and courts tend to use certain proxies for privacy in protecting citizens' privacy interests. In a sense, then, one can identify five modes of privacy that courts and legislatures focus upon in seeking to establish and preserve a sphere of privacy for citizens.

The first mode of privacy protection is space — *i.e.*, physical location. In particular, privacy protection can focus on particular places. Thus privacy law could provide protection by limiting physical intrusions upon individuals when in certain locations or, more generously, by specifying that activities taking place in particular locations are protected from outside interference (whether governmental or nongovernmental). For example, the law could establish "the home" as a place which neither law enforcement officers, regulators, journalists, nor potential non-media private intruders can enter without establishing probable cause to believe that illegal activities are occurring therein. The law might also provide that activities within the home are less subject to regulation or interference than they would be if conducted outside the home. We will see that the law indeed grants heightened protection to homes in ways that serve to protect privacy.

A second mode of privacy involves means of communications — privacy law could focus on protecting certain types of communications. Protecting communications from breach by outside parties might enable citizens to protect some of their confidences. In addition, particular methods of communicating might be especially highly valued and, thus, receive more rigorous protection than others. Thus, for instance, the law might provide heightened protection from intrusion for conversations conducted by telephone or in person. Though the means of communications might seem an odd proxy for privacy, sometimes both courts and legislatures have sought to protect particular means of communications.

A third mode of privacy protection focuses on controlling the means of intrusion. Under this approach, privacy is protected by restricting the use of some techniques employed to intrude into others' privacy. Thus, we might find that use of mechanical devices to record conversations is subject to special regulation because of the danger such conduct poses to privacy. Similarly, society might consider particularly troubling the use of polygraphs (and other devices used to measure physiological responses) or invasive surgical procedures to uncover relevant information about a person.⁶⁰ Thus, certain information might be sought

⁶⁰ *Schmerber v. California*, 384 U.S. 757, 770 (1966) (holding that intrusion into human body is particularly offensive and may only be undertaken upon "a clear indication that in

and disseminated, so long as an intruder does not employ a particularly troubling means of intrusion.

Fourth, privacy protection can focus on the subject-matter. Thus, courts and legislatures could establish privacy rules declaring certain types of information inappropriate for disclosure. For instance, a legislature might proscribe publication of the intimate details of sexual relationships or photographs of urination⁶¹ without the consent of the subject of the account or photograph. This fourth mode of privacy thus does not focus on protecting a specific physical location from intrusion or limiting the manner in which information is obtained.

Fifth, we might ground privacy in the protection of certain relationships. Some relationships might merit special legal protection — the doctor-patient and cleric-penitent relationships for example. Even if a relationship is unworthy of a conventional testimonial privilege, it might nevertheless warrant giving one or both of the parties to the relationship the power to exercise control over information imparted in the course of the relationship. Thus regulation using this fifth mode of privacy will seek to protect privacy by giving individuals some control over those with whom they share their private lives.

As I will discuss below, there is a sixth mode of privacy that is in some ways a combination of those outlined above. That mode of privacy focuses on databases and protects privacy by limiting access to and use of databases. The database mode of privacy merits at least brief exploration given the number of modern statutes that focus on database protection.

I will explore the manner in which various aspects of privacy law reflect each of the modes of privacy. I will also outline the difficulty that undercover operations pose with regard to statutes and common law doctrines embodying each of these

fact such evidence will be found"); *Winston v. Lee*, 470 U.S. 753, 767 (1985) ("A compelled surgical intrusion into an individual's body for evidence implicates expectations of privacy and security of such magnitude that the intrusion may be 'unreasonable' even if likely to produce evidence of a crime."); *Rochin v. California*, 342 U.S. 165 (1952) (holding that forcing a defendant to vomit two capsules of morphine that he had swallowed was a search in violation of his right to due process); see also Sherry F. Colb, *The Qualitative Dimension of Fourth Amendment Reasonableness*, 98 COLUM. L. REV. 1642, 1649–50 (1998) (noting that courts have held that probable cause and warrants are not by themselves sufficient to justify a surgical search).

⁶¹ *Skinner v. Railway Labor Executives Ass'n*, 489 U.S. 602, 617 (1989); *Haynes v. Alfred Knopf*, 8 F.3d 1222, 1229 (7th Cir. 1993); *Nat'l Treasury Employees Union v. Von Raab*, 816 F.2d 170, 175 (5th Cir. 1987) ("There are few activities in our society more personal and private than the passing of urine. . . . It is a function traditionally performed without public observations; indeed its performance in public is generally prohibited by law as well as social custom."), *aff'd in part, vacated in part on other grounds*, 489 U.S. 656 (1989); *Daily Times Democrat v. Graham*, 162 So.2d 474 (Ala. 1964) (involving "indecent exposure," namely the revealing of the underwear of woman whose clothes were unexpectedly blown up by air vents).

modes of privacy.

A. Physical Location as a Mode of Privacy

The primary protections against potential governmental and nongovernmental intruders focus on physical location. The U.S. Supreme Court's Fourth Amendment jurisprudence has, until relatively recently, focused on real property concepts.⁶² As some have noted critically, privacy receives protection because real property — most particularly the right to exclude others from private property — receives protection.⁶³ If a person lacks property interests, that person probably can secure little privacy. Concomitantly, the more property one possesses, the greater one's opportunity to secure privacy. Indeed, the Supreme Court's focus on property in defining privacy rights was so pronounced that the Court felt compelled to make clear in *Katz v. United States*,⁶⁴ and repeatedly thereafter, that the Fourth Amendment "protects people, not places."⁶⁵ The Fourth Amendment, and thus the Court's property-focused interpretation of that Amendment, governs both investigatory searches and regulatory searches. Albeit, the Court has crafted an exception to the warrant and probable cause requirement that sometimes allows regulators to intrude upon private real property without probable cause or a warrant.⁶⁶

Location-based privacy approaches defining the scope of privacy need not exclusively turn on real property interests. For example, use of hidden cameras in public bathroom stalls constitutes a search requiring probable cause and a warrant (or the equivalent) because users of such facilities possess a reasonable expectation of privacy in the stall while they occupy it, regardless of their lack of any real property claim to dominion over the stall.⁶⁷ Similarly, in a few circumstances, a

⁶² See *Kyllo v. United States*, 533 U.S. 27, 31 (2001) ("[O]ur Fourth Amendment jurisprudence was tied to common-law trespass.").

⁶³ E.g., HANNAH ARENDT, *THE HUMAN CONDITION* 38–78 (1958) ("The only efficient way to guarantee the darkness of what needs to be hidden against the light of publicity is private property, a privately owned place to hide in.").

⁶⁴ 389 U.S. 347 (1967).

⁶⁵ *Id.* at 351. However, real property rights do not fully define the expectation of privacy. Thus, in the context of police intrusions into open fields owned by a private individual, the Court has declared that the law of trespass confers protections from intrusion broader than the protections offered by the Fourth Amendment. Thus, the Court held, law enforcement officials may trespass on real property without violating any reasonable expectation of privacy and, accordingly, law enforcement officials need neither a warrant nor probable cause to enter an open field. *Oliver v. United States*, 466 U.S. 170, 183–84 & n.15 (1984).

⁶⁶ Thus, the Court recognizes an entitlement to privacy based on property ownership but allows law enforcement to frustrate the legitimate privacy expectation by means other than the traditional manner of the issuance of a warrant and/or the existence of probable cause.

⁶⁷ *People v. Dezek*, 308 N.W.2d 652, 655 (Mich. Ct. App. 1981) (recognizing privacy

person may own property but lack a reasonable expectation of privacy that precludes others from entering the property to observe them.⁶⁸

Courts have employed similar property-based privacy approach with regard to private intruders: the intruder's physical location is often central to intrusion against seclusion claims.⁶⁹ If a journalist obtains personal information about a person while in a place open to the public, the aggrieved individual ordinarily cannot prevail on a privacy claim.⁷⁰ However, if the journalist is in an area barred from the general public, gathering personal information can form the grounds of liability.⁷¹ A location may be unavailable to the public for several reasons, but often such inaccessibility results from private property owners exercising their power to exclude. Thus, the intrusion into seclusion cause of action may offer limited privacy protection because private areas may be somewhat accessible to people who remain in public areas and use their natural or mechanically enhanced powers of observation. Moreover, the location-focused quality of common-law intrusion claims makes extremely difficult successful assertion of a privacy cause of action against extensive and intrusive monitoring that occurs in public places.⁷²

interest in rest stop stalls during periods of occupation); *State v. Casconi*, 766 P.2d 397, 399 (Or. Ct. App. 1988) ("The final bastion of privacy is to be found in the area of human procreation and excretion" and "[i]f a person was entitled to any shred of privacy, then it is to privacy in these matters.") (quoting *Sterling v. Cupp*, 607 P.2d 206 (Or. Ct. App. 1980) (decided under Oregon state constitution). See generally Michael R. Flaherty, Annotation, *Search and Seizure: Reasonable Expectation of Privacy in Public Restroom*, 74 A.L.R.4TH 508 (1989) (discussing judicial treatment of claims to privacy in public restrooms).

⁶⁸ See *supra* note 65.

⁶⁹ Bell, *supra* note 11, at 767 & nn.95-97.

⁷⁰ See *Shulman v. Group W Productions, Inc.*, 955 P.2d 469, 490-92 (Cal. 1998) ("The tort [of intrusion] is proven only if the plaintiff had an objectively reasonable expectation of seclusion or solitude in the place . . ."); see also *People for the Ethical Treatment of Animals v. Bobby Berossini, Ltd.*, 895 P.2d 1269, 1280-81 & n.20 (Nev. 1995); Andrew Jay McClurg, *Bringing Privacy Law Out of the Closet: A Tort Theor of Liability for Intrusions in Public Places*, 73 N.C. L. REV. 989, 1036-41 (1995). See generally C. THOMAS DIENES ET AL., *NEWSGATHERING AND THE LAW* §§ 12-2, 12-4(c)(2) (2d ed. 1997).

⁷¹ See, e.g., *Shulman*, 955 P.2d at 492. For instance, when deciding whether journalists had tortiously intruded upon an accident victim, the *Shulman* court focused on the observations that could be made from the highway, the presence of any bystanders at the accident scene, and the statements such bystanders could hear. See *Shulman*, 955 P.2d at 491; see also *Miller v. Nat'l Broad. Co.*, 232 Cal. Rptr. 668, 677-78, 684-85 (Cal. Ct. App. 1986) (allowing plaintiff's claim against a television crew who entered her home without permission to film emergency personnel attempting to revive her husband).

⁷² See *Nader v. Gen. Motors Corp.*, 255 N.E.2d 765 (N.Y. 1970).

A few cases have been successful, but often because the surveillance was visible. Such visible surveillance adds an element of harassment and intimidation to the public scrutiny. See, e.g., *Galella v. Onassis*, 487 F.2d 986, 994 & n.11, 995 (2d Cir. 1973) (recognizing an implied right of action against paparazzi for violating criminal harassment statute); *Wolfson v. Lewis*, 924 F. Supp. 1413, 1435 (E.D. Pa. 1995) (enjoining reporters from "harassing,

A well-known case, *Nader v. General Motors Corp.*,⁷³ illustrates the difficulty of prevailing upon an intrusion claim arising from public surveillance. The case involved wide-ranging allegations that General Motors had harassed consumer advocate Ralph Nader. Nader alleged that General Motors “hired people to shadow [him] and keep him under surveillance.” On one occasion, he claimed, his General Motors “shadow” followed him sufficiently closely to observe “the denomination

hounding, following, intruding, frightening, terrorizing, or ambushing” certain corporate executives whose salaries the reporters were investigating); *Pinkerton Nat’l Detective Agency, Inc. v. Stevens*, 132 S.E.2d 119, 122–23 (Ga. Ct. App. 1963) (affirming claim of invasion of privacy where neighbors’ opinions of the plaintiff were negatively affected by witnessing the defendant’s constant investigation of the plaintiff); *Le Mistral v. Columbia Broad. Sys.*, 402 N.Y.S.2d 815, 816 n.1, 817 (N.Y. App. Div. 1978) (affirming jury verdict against television station that sent a camera crew into an upscale restaurant without permission, alarming patrons); *Schultz v. Frankfort Marine Accident & Plate Glass Ins. Co.*, 139 N.W. 386, 389–90 (Wis. 1913) (finding “open or rough shadowing” to be defamatory); RESTATEMENT (SECOND) OF TORTS § 652B cmt. d (1977) (stating that an intrusion may arise from a “course of hounding the plaintiff”). For a proposal to develop a cause of action for privacy even in a public place, see McClurg, *supra* note 70, at 1055–59.

Similarly, it is hard to make out a claim against law enforcement officers’ surreptitious use of facial recognition technology in public places because anyone who is scanned is in open public. See Dana Canedy, *Tampa Scans the Faces in Its Crowd for Criminals*, N.Y. TIMES, July 4, 2001, at A1. However, at least prior to September 11, 2001, there was a chorus of criticism over the use of video monitors and face recognition technology to identify people on public streets. Ross Kerber, *Technology & Innovation: Face-Recognition Software Spurs Privacy Fears*, BOSTON GLOBE, Aug. 20, 2001, at C1; Miki Meek, *You Can’t Hide Those Lying Eyes in Tampa: Street Cameras Spark a Privacy Debate*, U.S. NEWS & WORLD REP., Aug. 6, 2001, at 20; Rick Montgomery, *Face-Recognition Software Getting a Hard Look Since Sept. 11*, KANSAS CITY STAR, Nov. 25 2001, at A1; Robert O’Harrow Jr., *Matching Faces With Mug Shots; Software for Police, Others Stirs Privacy Concerns*, WASH. POST, Aug. 1, 2001, at A1.

The discomfort with face scans in public street may be explained, in part, by the asymmetry in positions of the various actors involved. The watched, *i.e.*, citizens using the streets, cannot observe the watcher. If a real person is doing the watching, individuals using that public place may at least determine when the watcher has focused upon them. In addition, the watcher runs the risk that the object of his interest may subject him to the same treatment. Also, individuals being watched by an actual person may confront the watcher and ask what he is doing and why; if done in a sufficiently public place, such a confrontation might enlist the help of others nearby. This qualitative difference between real-person and mechanized surveillance has not prevented the Supreme Court from equating the two forms of surveillance. See *United States v. Knotts*, 460 U.S. 276, 281–83 (1983) (treating surveillance of a vehicle via a secretly planted transmitter as the equivalent of surveillance by actual people along the vehicle’s route).

Moreover, face-recognition technology has the potential for invading people’s “space.” A camera operator using zoom technology could focus in on details observable by the naked eye only if the observer were staring intently at the person watched from inches away.

⁷³ 255 N.E.2d 765 (N.Y. 1970).

of the bills he was withdrawing from his account.”⁷⁴ The court explained that

[a] person does not automatically make public everything he does merely by being in a public place, and the mere fact that Nader was in a bank did not give anyone the right to try to discover the amount of money he was withdrawing. On the other hand, if plaintiff acted in such a way as to reveal [the] facts to any casual observer, then, it may not be said that the appellant intruded into his private sphere.⁷⁵

Though the court phrased its analysis in terms of the subject matter to which intruders may direct their attention, by suggesting that information regarding the amount of a person’s withdrawals from his bank account is a private matter, suggesting that the court really adopts a location-based analysis. In *Nader*, as in the public bathroom cases mentioned earlier, the location-focused analysis does not turn on strict application of property concepts. As the court explained, even in a public place we may have a small area around us that social custom defines as ours, and that we may ask others to keep inviolate.⁷⁶ Among other things, such personal space enables individuals to access purses or wallets that contain personal, private matters without revealing those matters to others. If the subject matter, withdrawal of money from a bank, were truly the crux of the *Nader* court’s analysis, a casual observer who could see the denominations of the currency Nader was withdrawing because of Nader’s carelessness in failing to keep the currency from sight could neither stare at Nader to discover the denominations of the currency Nader held nor communicate information about Nader’s withdrawal of money (even that gained from casual observation). The *Nader* Court surely did not intend to establish such a principle.

From another perspective too, physical space often assumes central importance in privacy law. Courts (or legislatures) may sometimes characterize conduct as public or private depending on the nature of the location in which that conduct occurs.⁷⁷ For example, in *Stanley v. Georgia*,⁷⁸ the Supreme Court precluded the

⁷⁴ *Id.* at 771.

⁷⁵ *Id.*

⁷⁶ See *id.* See generally Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 971–74 (1989) (discussing the role of the social construct of private space in shaping intrusion law).

⁷⁷ *Stanley v. Georgia*, 394 U.S. 557, 565 (1969) (“[A] state has no business telling a man sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men’s minds.”).

Indeed, the Court invalidated contraception laws, in part, because enforcement of such statutes would require law enforcement officials to invade “the sacred precincts of marital bedrooms.” *Griswold v. Connecticut*, 381 U.S. 479, 485–86 (1965) (“Would we allow the

government from enforcing laws prohibiting possession of obscene material against a man who held such proscribed obscenity within the confines of his home. The Court held that the government could generally prohibit possession of obscene materials outside of the home and could punish acquisition of such materials — even if intended for use in the home — but could not prosecute the homeowner for possession once he brought the contraband inside his home.⁷⁹ As the Court explained, “whatever may be the justification for other statutes regulating obscenity, we do not think they reach into the privacy of one’s own home.”⁸⁰

The controversial Alaska Supreme Court decision in *Ravin v. State*⁸¹ provides a second example of a judicial determination that otherwise illegal activity may become constitutionally protected private conduct because it occurs within the home. In *Ravin*, the court held that, even though the state may prohibit possession and the purchase and sale of marijuana in general, the government may not prosecute an individual for consuming marijuana at home.⁸² The court based its decision on the Alaska Constitution’s right of privacy clause, finding that the clause protected consumption of marijuana so long as it occurred in one’s home.⁸³ This view that conduct more easily qualifies as private if it occurs within the home may explain the reaction, hyperbolically described as “global ridicule,” to a Friendship

police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marital relationship.”); *id.* at 495 (Goldberg, J., concurring) (“The Connecticut statutes here involved deal with a particularly important and sensitive area of privacy — that of the marital relationship and the *marital home*.”) (emphasis added). Of course, this argument was not solely rooted in place but was also rooted in protection of a special relationship, namely that of husband and wife. *See Stuntz, supra* note 7, at 1026 n.43.

⁷⁸ 394 U.S. 557 (1969).

⁷⁹ *Id.* at 568.

⁸⁰ *Id.* at 565.

⁸¹ 537 P.2d 494 (Alaska 1975).

⁸² *Id.* at 511.

⁸³ *Id.* at 504. *Compare* *Robinson v. California*, 370 U.S. 660, 676–77 (1962) (declaring unconstitutional a law criminalizing narcotics addiction), *with* *Powell v. Texas*, 392 U.S. 514, 532–37 (1968) (refusing to extend the *Robinson* holding to punishment of a chronic alcoholic for public drunkenness, in part because Texas had not “attempted to regulate appellant’s behavior in the privacy of his own home”). *But see* *Bowers v. Hardwick*, 478 U.S. 186, 195 (1986) (“Plainly enough, otherwise illegal conduct is not immunized whenever it occurs in the home. Victimless crimes, such as the possession or use of illegal drugs, do not escape the law where they are committed at home.”).

However, when the conduct a resident engages in at home becomes commercialized, courts often consider the conduct to have been transformed from “private” to “public.” *See, e.g., State v. Mueller*, 671 P.2d 1351, 1360 (1983) (holding that prostitution occurring within a private residence is not protected by Hawaii’s constitutional right of privacy). *Compare Ravin*, 537 P.2d at 511, *with*, *Belgarde v. State*, 543 P.2d 206 (Alaska 1975) (commercial sale of narcotics to another in home not protected by the Alaska right of privacy).

Heights, Maryland ordinance banning smoking at home if secondary smoke escapes the home and poses health risks to those outside.⁸⁴

Thus, certain places receive a heightened, but not absolute, privacy protections. As suggested above, the home has traditionally been the place where privacy interests are strongest.⁸⁵ Perhaps the home receives such heightened protection because of the types of activities individuals tend to engage in at home. Many of the most private aspects of life take place in, or are at least centered around, residences. Moreover, the home is the locus of personal life rather than commercial life. Courts justifiably tend to view commercial life as less private; therefore, courts accord commercial enterprises far less robust Fourth Amendment protection.⁸⁶ Much of the more limited Fourth Amendment protection in the regulatory environment stems from the commercial nature of the typical premises subject to regulatory intrusions.⁸⁷

⁸⁴ Jo Becker, *Global Ridicule Extinguishes Montgomery's Anti-Smoking Bill*, WASH. POST, Nov. 28, 2001, at A1; Jo Becker, *Smokers Told to Fetter Their Fumes*, WASH. POST, Nov. 21, 2001, at A1.

Similarly, those who visit a residence, as opposed to a business establishment, have less of a right to impose upon their hosts the obligation to keep the premises free from physical hazards. Thus, visitors to a commercial establishments' public areas and individuals invited onto premises for commercial purposes qualify as "invitees" and have a right to expect landowners to exercise reasonable care. RESTATEMENT (SECOND) OF TORTS § 332 (1977). Social guests to residences, however, must take the premises as they find them, and the host ordinarily must merely disclose dangerous conditions. *Id.* at § 342. Granted, several jurisdictions have jettisoned the rigidity of this traditional approach. Nevertheless, landowners' freedom to act on their own property despite the risk of injury to those who come onto their land is unusually pronounced when the property is a private residence. *Compare id.*, with *id.* at § 332. Generally, the duty to avoid reasonably foreseeable harm to others is much greater than the duty the law imposes on landowners with regard to social visitors. *Id.* at § 342.

⁸⁵ See *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (requiring a search warrant to support thermal scanning of a home); *Payton v. New York*, 445 U.S. 573, 589–90 (1980) (asserting that being arrested in your home is such a substantial invasion that a warrant is required, unless there are exigent circumstances); NELSON LASSON, *THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION* 13–15 (1970). See generally LAFAVE ET AL., *supra* note 20, § 3.2(c); Jonathan L. Hafetz, "A Man's Home is his Castle?: Reflections on the Home, the Family, and Privacy During the Late Nineteenth and Early Twentieth Centuries," 8 WM. & MARY J. WOMEN & L. 175, 175–183 (2002).

⁸⁶ See *Dow Chemical Co. v. U.S.*, 476 U.S. 227, 235–39, 237 n.4 (1986) (allowing aerial surveillance of large industrial complex, but suggesting that the result would be different as to "an area immediately adjacent to a private home, where privacy expectations are most heightened").

⁸⁷ Administrative searches, however, are not invariably limited to businesses. See *Camara v. Municipal Court*, 387 U.S. 523 (1967); *Frank v. State*, 359 U.S. 360 (1959).

Some nonresidential locations receive heightened protection, in part to protect privacy

Undercover techniques defeat location-based protection to the extent that location-based protection focuses on ensuring that owners control physical access to their property.⁸⁸ The inefficacy of location-based protection against undercover intruders stems from such intruders' use of deception rather than coercion. The intruder uses deception to obtain the property owner's consent to enter her property, and consent is a standard defense to Fourth Amendment and common-law trespass claims.⁸⁹ Courts could hold that deception vitiates such consent in general.⁹⁰ While

interests. Thus, the Supreme Court has recognized the importance of the sanctity of newsrooms. While refusing to accord newsrooms special protections, the Court has specified that law enforcement officials may search newsrooms for evidence of crimes committed by third parties only if they observe the Fourth Amendment with "scrupulous exactitude." *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (quoting *Stanford v. Texas*, 379 U.S. 476, 485 (1965)). In response to the limited protections the Court established in *Zurcher*, Congress enacted a statute which provided more protection by further limiting law enforcement searches of newsrooms. Privacy Protection Act of 1980, Pub. L. No. 96-440, 94 Stat. 1879 (codified at 42 U.S.C. § 2000aa (1994)). Some states have gone even farther still in protecting newsrooms. MARC A. FRANKLIN ET AL., *MASS MEDIA LAW: CASES AND MATERIALS* 665-66 (6th ed. 2000) (describing state statutory response to *Zurcher*). Admittedly, the impetus for severely restricting newsroom searches is not really journalists' privacy concerns, but the detrimental effects such searches have on journalists' ability to gather and disseminate news.

⁸⁸ Individual claims of breach of physical privacy by deception often challenge residential intrusions. However, some cases have involved individuals' claims of privacy in their office space. In *State v. Hayes*, the plaintiff argued that the due process clauses of the federal and Vermont constitutions prohibit the government from conducting undercover investigations in private workplaces absent a reason to believe that illegal activity is afoot. *State v. Hayes*, 752 A.2d 16, 18 (Vt. 2000). The Court rejected the argument, relying on a consent rationale. See also *Sanders v. Am. Broad. Cos.*, 978 P.2d 67 (Cal. 1999).

Technological advance can have a similar effect because it allows law enforcement officers to penetrate physical boundaries and physical space. See *infra* note 104.

⁸⁹ *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973); RESTATEMENT (SECOND) OF TORTS § 892A(1) (1979) ("One who effectively consents to conduct of another intended to invade his interest cannot recover in an action of tort for the conduct or for harm resulting from it."); *id.* § 167-175 (addressing the effect of consent in trespass claims); see also LAFAVE ET AL., *supra* note 20, § 3.10.

⁹⁰ Indeed, the Restatement of Torts suggests that an actor's consent has not effect if given based on the recipient's misrepresentation of the nature of the consenter's interest being invaded or the harm expected as a result. RESTATEMENT (SECOND) OF TORTS § 892B (1979). The courts have not applied this approach to trespass claims involving journalists. Judge Posner discusses the Restatement in *Desnick v. American Broadcasting Companies* and concludes that the deception in that case did not interfere with the interest that the tort of trespass is designed to protect. *Desnick v. Am. Broad. Co.*, 44 F.3d 1345, 1352 (7th Cir. 1995).

No embarrassingly intimate details of anybody's life were publicized in the present case. There was no eavesdropping on a private conversation; the testers recorded their own conversations with the Desnick Eye Center's physicians.

a knowing and intelligent waiver of constitutional rights is permissible, waiver under a misimpression might not be. The constitutional limitations on judicial acceptance of guilty pleas and police interrogation illustrate the principle. A court may accept a defendant's guilty plea only after conducting a lengthy plea allocution, during which the judge ensures that the defendant understands the rights being renounced.⁹¹ Police interrogations must be preceded by a *Miranda* warning if the subject is the target of the investigation.⁹² Courts could employ a similar approach to constrain investigators' physical intrusions.⁹³ For reasons that I will discuss later,⁹⁴ courts have abjured that approach when addressing both governmental and nongovernmental intrusions.⁹⁵

There was no violation of the doctor-patient privilege. There was no theft, or intent to steal, trade secrets; no disruption of decorum, of peace and quiet; no noisy or distracting demonstrations.

Id. Note that Posner's analysis in *Desnick* touches upon almost all of the modes of privacy discussed herein: physical location (no invasion of "private space"), means of communication (no eavesdropping on private conversation), means of intrusion (no disruption of decorum), subject matter (no publicizing of embarrassingly intimate details of anybody's life), and relationships (no violation of the doctor-patient privilege).

Posner suggests more generally that judicially permitted deceptions often can be viewed as not vitiating the interest protected by the tort cause of actions that plaintiffs seek to assert. *Id.*

⁹¹ LAFAYE ET AL., *supra* note 20 at § 20.4(b)-(e).

⁹² *Id.* §§ 6.5, 6.8; *see also* *United States v. Henry*, 447 U.S. 264 (1980) (holding that waiver of the right to counsel cannot be established where the defendant spoke with an undisclosed undercover informant because waiver is valid only if defendant is aware that he is waiving his right to counsel before "a [g]overnment agent expressly commissioned to secure evidence"); *Rhode Island v. Innis*, 446 U.S. 291 (1980) (holding that police did not violate a defendant's *Miranda* rights when the defendant voluntarily revealed the location of a weapon to police after he was read his rights). Although, as some have pointed out, deception is not eliminated in the police interrogation situation even with regard to *Miranda* warnings, *see* Christopher Slobogin, *Deceit, Pretext, and Trickery: Investigative Lies by the Police*, 76 OR. L. REV. 775, 785-88 (1997), *Miranda* does establish some requirement of a knowing and intelligent waiver of rights. At least in the interrogation context, the suspect knows he is interacting with the police; in the undercover setting, the target of the operation will not even know that, and in fact, deception as to that fact is essential to undercover work.

⁹³ *See* Lloyd L. Weinreb, *Generalities of the Fourth Amendment*, 42 U. CHI. L. REV. 47, 67 (1974).

⁹⁴ *See infra* note 180 for a discussion of confidential relationships.

⁹⁵ *United States v. White*, 401 U.S. 745 (1971) (holding that evidence obtained through a government informant and the use of a radio transmitter did not violate the Fourth Amendment); *Hoffa v. United States*, 385 U.S. 293 (1966) (upholding the validity of evidence obtained through use of a paid government informant); *Lee v. United States*, 343 U.S. 747 (1952) (holding that evidence obtained by an undercover agent with a concealed radio transmitter was valid and not obtained by trespass); *see also* *Lopez v. United States*, 373 U.S. 427 (1963); *Food Lion, Inc. v. Capital Cities/ABC, Inc.*, 194 F.3d 505 (4th Cir. 1999); *Dietemann v. Time, Inc.*, 449 F.2d 245 (9th Cir. 1971).

Interestingly, in *United States v. Lewis*,⁹⁶ the case allowing undercover officers to operate in homes, despite fraudulently gaining the homeowner's consent to enter, the Court justified its conclusion that the officers' conduct did not violate the homeowner's Fourth Amendment right to privacy by noting that the residence had become a locus of commerce. In short, defendant was essentially using his residence to conduct commercial activity.⁹⁷ However, courts have not narrowly interpreted *Lewis*, and the other Supreme Court cases upholding undercover investigations, to authorize undercover entry of residences only pursuant to investigations of commercial activity.⁹⁸ Thus, courts have not suggested that law enforcement may not use deception to enter a home when investigating merely personal, non-commercial crimes.

Undercover techniques need not defeat location-based privacy protection if such location-based protection prohibited government acquisition of information regarding a place receiving heightened protection, like a residential interior, even if acquisition of the information does not required physical intrusion. Indeed, the Court's recent decision in *Kyllo v. United States*⁹⁹ tentatively suggests that the home may be protected even when property rules permitting owners to deny physical access cannot shield residential interiors. The *Kyllo* majority suggests that, even if police wish to use technical devices while outside a person's property, they may not

United States v. Karo, 468 U.S. 705 (1984), provides one exception, albeit in a different context. In *Karo*, police officers monitored a beeper that emitted a special electronic signal indicating the opening of the container in which it was lodged. The container was opened inside a residence, and the Court held that law enforcement officers could not monitor the beeper for the special signals while the object containing the beeper remained in a residence. *Id.* at 714. The police officers could establish consent, at least in a broad sense. The defendant had voluntarily acquired the beeper-laden article, and thus a strong "assumption of the risk" argument could be advanced. See *id.* at 724 (O'Connor, J., concurring). The Court rejected that approach, explaining that the beeper conveyed information about events that took place within the protected property, *i.e.*, the residence. *Id.* at 714-16 & n.4. The Court found insignificant two facts that would normally hold great significance: first, that the beeper was monitored from a public place — and so there was no physical breach of a protected location by the officers, and second, that any breach resulted from the target's own act of bringing the beeper onto his property. *Id.*

⁹⁶ 385 U.S. 206 (1966).

⁹⁷ *Id.* at 213 ("But when, as here, the home is converted into a commercial center to which outsiders are invited for purposes of transacting unlawful business, that business is entitled to no greater sanctity than if it were carried on in a store, a garage, a car, or on the street. A government agent, in the same manner as a private person, may accept an invitation to do business and may enter upon the premises for the very purposes contemplated by the occupant.").

⁹⁸ Indeed, some courts suggest that *Lewis* holds that the homeowner loses the enhanced privacy rights associated with residences only when he indicates a willingness to engage in an illegal transaction. See *State v. Hayes*, 752 A.2d 16 (Vt. 2000).

⁹⁹ 533 U.S. 27 (2001).

do so if the device reveals information about the interior of the home that they could otherwise obtain only by a physical intrusion. The Court limited its holding to devices not generally in public use.¹⁰⁰

Kyllo involved police use of thermal imaging units that could identify unusual heat sources within buildings. As currently used, such devices reveal little information other than the homeowner's criminal activity — principally they are used to uncover homeowners cultivation of marijuana (which may explain the limited use of such devices by the general public that the Court found so critical).¹⁰¹ Undercover officers, and confidential informants operating under government direction acquire a far broader range of information, information regarding far more than illegal conduct.

Nevertheless, *Kyllo* will probably not lead any court to conclude that the privacy interest in homes prohibits undercover operations that could detect matters that could not be detected by one outside the home requires probable cause, a warrant, or any type of individualized suspicion.¹⁰² Such a rule would make

¹⁰⁰ The *Kyllo* Court explained:

To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment. We think 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.

Id. at 34 (quoting *Silverman v. United States*, 365 U.S. 505, 512 (1961)) (citation omitted).

The Court's general approach to mechanical enhancements of unaided human senses has been criticized as inconsistent. See David E. Steinberg, *Making Sense of Sense-Enhanced Searches*, 74 MINN. L. REV. 563 (1990). See generally LAFAYETTE ET AL., *supra* note 20, § 3.2(b). The Court asserts that the test is whether the mechanical device is in common use. *Dow Chemical Co. v. United States*, 476 U.S. 227, 231 (1986). But see CLIFFORD S. FISHMAN & ANNE T. MCKENNA, *WIRETAPPING AND EAVESDROPPING* § 29:16, at 29–30 & n.7 (2d ed. 1995) (observing that, under the Court's own test, *Dow Chemical* should have come out the other way because satellite photograph is available to private news organizations).

Statutes should have some effect on this determination. Some statutes prohibit the use of devices that can be used to intrude. For example, federal law prohibits the public sale of devices facilitating surreptitious interception of wire, oral or electronic communications. 18 U.S.C. § 2512 (2000).

¹⁰¹ See generally *United States v. Place*, 462 U.S. 696 (1983), which approved the practice of subjecting luggage to drug-sniffing dogs because the dogs revealed only the presence of contraband. Thus such dog sniffs focused only on illegal activity. They were not over-inclusive — *i.e.*, they did not tell law enforcement officials about legal property the bag's owner possessed.

¹⁰² *United States v. Davis*, — F.3d —, 2003 WL 1908025 (2d Cir. Apr. 22, 2003) (dismissing argument that undercover use of video recording equipment while in defendant's

undercover work in the decidedly blue-collar area of drug enforcement impractical: Agents might have to avoid entering homes until they could get a warrant, and as a result, deprive agents of the flexibility needed for undercover operations.¹⁰³

In short, in the criminal, regulatory and civil context, location has played a central role in protecting privacy both by giving individuals a physical area from which they can exclude the curious and by defining privacy in terms of the location in which an activity takes place. This location-based approach has not adequately protected privacy, and absent a drastic change of judicial approach, undercover operations will continue to undermine such location-based protections.

B. The Means of Communication as a Mode of Privacy

Society might choose to protect privacy by protecting all, or at least some, means of communication from unwanted breach rather than by protecting certain physical locations. Thus, for example, rather than protecting the place in which speakers engage in communication, protection would focus on shielding the communication itself, rendering the speakers' or potential intruder's location irrelevant.¹⁰⁴

The question of whether wiretapping constitutes an invasion of privacy exemplifies the radical divergence between location-focused and means-of-communications-focused definitions of privacy — and the court's location-focused analysis lies at the root of its historically inadequate analysis of wiretapping. If

home to consummate a drug transaction made unconstitutional by *Kyllo*).

¹⁰³ See Philip B. Heymann, *Understanding Criminal Investigations*, 22 HARV. J. ON LEGIS. 315, 331–34 (1985); see also *FBI Undercover Guidelines: Oversight Hearings Before the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary*, 97th Cong. 83–84, 106 (1981) (testimony of Associate Attorney General Paul R. Michel) (explaining that requiring probable cause or reasonable suspicion before an undercover officer offers a person an opportunity to commit a crime is unworkable because undercover investigations “are inherently and unavoidably evolutionary in nature”); MARX, *supra* note 8, at 195; Bell, *supra* note 11, at 799 n.235 (“Establishing standards for undercover operators is particularly troublesome, in part due to the fluidity of many undercover situations. Even police officials supervising undercover operations have trouble drawing lines and providing firm instructions given the necessary fluidity of the situation”); Katherine Goldwasser, *After ABSCAM: An Examination of Congressional Proposals to Limit Targeting Discretion in Federal Undercover Investigations*, 36 EMORY L.J. 75, 128–29 (1987).

¹⁰⁴ Location-based privacy rules can partially protect the means of communication, particularly if the communication involves face-to-face contact. However, technological advances even erode location-based protections of face-to-face communications. More significantly, much of modern communication does not take place in person, but rather by means of communication that rely upon channels open to the general public. Most mail goes through a federal instrumentality itself. Telephonic and electronic communications are transmitted by common carriers.

analyzed employing a location-focused perspective, wiretapping may not constitute a "search or seizure" if the wiretapper merely reaches the telephone company's property.¹⁰⁵ More specifically, had the Court employed its traditional location-focused analysis, in *Katz v. United States*, it would have rejected Katz's Fourth Amendment claim¹⁰⁶ because a telephone booth from which Katz placed his call was not a protected place under traditional Fourth Amendment analysis: a law enforcement officer, or anyone else, could view Katz through the glass of the phone booth.¹⁰⁷ Indeed, until *Katz* the Court had focused on constitutionally protected areas.¹⁰⁸ But the breakthrough that made *Katz* a seminal case was the Court's focus on the means of communication — in particular, whether telephone communications deserved protection, rather than on the location of the participant in the phone conversation.¹⁰⁹ Though the phone booth Katz had used was not itself a constitutionally protected place, Katz could assert a legitimate expectation of privacy in the contents of his conversation because the conversation had taken place over the telephone.¹¹⁰

¹⁰⁵ *Olmstead v. United States*, 277 U.S. 438 (1928). Thus, for example, the government does not breach any reasonable expectation of privacy, and thus does not conduct a search or seizure, if it convinces the telephone company to install a pen register on a subscriber's line. *Smith v. Maryland*, 442 U.S. 735 (1979).

¹⁰⁶ Indeed, the question presented as the petitioner formulated it was "whether a public telephone booth is a constitutionally protected area . . . ?" *Katz v. United States*, 389 U.S. 347, 349 (1967). Interestingly, the second question focused on whether the existence of a trespass was of critical Fourth Amendment importance.

¹⁰⁷ A court could designate telephone booths as protected places because of the nature of the activity that customarily occurs therein — namely personal telephone conversations that the speaker expects to remain private. Thus, a nonconventional property-focused analysis might have accorded Katz an expectation of privacy by precluding law enforcement officials from penetrating that booth, either physically or by electronic means, without satisfying the Fourth Amendment's warrant and probable cause requirements.

¹⁰⁸ LAFAVE ET AL., *supra* note 20, § 3.2(a), at 133; RICHARD C. TURKINGTON & ANITA L. ALLEN, *PRIVACY LAW: CASES AND MATERIALS* 92 (1999).

¹⁰⁹ *Katz*, 389 U.S. at 352 ("To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.").

¹¹⁰ The Supreme Court had long before taken an analogous approach to the mails. See *Ex Parte Jackson*, 96 U.S. 727 (1877) (holding unconstitutional postal officials' opening and reading of sealed letters); see also *Olmstead*, 277 U.S. at 464 (distinguishing sealed letters from telephone conversations). The constitutional protection has been supplemented by administrative regulations limiting the use of "mail covers." In a "mail cover," postal employees record the information on the outside of envelopes mailed by a particular patron. Law enforcement officers cannot obtain authorization for a mail cover unless they establish reason to believe that the mail cover will provide evidence of a serious crime or lead to the apprehension of a fugitive. See 39 C.F.R. § 233.3 (2002); see also JAMES RULE ET AL., *THE POLITICS OF PRIVACY: PLANNING FOR PERSONAL DATA SYSTEMS AS POWERFUL TECHNOLOGIES* 55 (1980).

The law regarding mail covers provides an example of situations in which nonjudicial

No means of communication can be absolutely immune from breach. Such absolute immunity would create a means for conspirators to plot and carry out crimes free from government scrutiny. Some advocates of encryption have argued that Internet communications should essentially be absolutely immune from breach.¹¹¹ By contrast, law enforcement agencies seek built-in "back doors" permitting decryption of encrypted messages. Such back doors would allow law enforcement access to the encrypted messages upon a showing of probable cause.¹¹²

Wiretap laws were crafted to protect privacy by safeguarding the means many

entities are more privacy-protective than courts. Courts have not restricted mail covers.

Lower courts have rarely perceived that any interest protected by the fourth amendment is implicated by mail covers. In part, this is due to recurring attacks of Olmsteadism: no trespass is involved, no search or seizure occurs when the eye registers the impressions from the outside of an envelope or the hand records the information. . . . Equally rare is recognition that "the mails [are] almost as much a part of free speech as the right to use our tongues"

Shirley M. Hufstедler, *Invisible Searches for Intangible Things: Regulation of Governmental Information Gathering*, 127 U. PA. L. REV. 1483, 1510–11 (1979) (quoting *United States ex rel. Milwaukee Social Democratic Publ'g Co. v. Burleson*, 255 U.S. 407, 437 (1921)) (citation omitted) (alteration in original); see also Sandy D. Hellums, Note, *Bits and Bytes: The Carnivore Initiative and the Search and Seizure of Electronic Mail*, 10 WM. & MARY BILL RTS. J. 827, 837–39 (2001) (discussing the Supreme Court's upholding of mail covers as constitutional in *United States v. Jacobson*, 466 U.S. 109 (1983)); *Invasion of Privacy: Use and Abuse of Mail Covers*, 4 COLUM. J.L. & SOC. PROBS. 165 (1968).

¹¹¹ Often, technological advances tend to reduce privacy. *Olmstead*, 277 U.S. at 473–74 (Brandeis, J., dissenting); see also *Kyllo v. United States*, 533 U.S. 27 (2001); TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 203 (Philip E. Agre & Marc Rotenberg eds., 1998). But encryption is a privacy-enhancing technological advance. See MARX, *supra* note 8, at 217–19.

¹¹² [K]ey recovery is basically an updated tap. To argue that the government is permitted to tape regular phone calls, even if the callers are using some kind of coded language . . . , but not to eavesdrop on encrypted messages is no more logical than to suggest that the government may search and seize old-fashioned paper files (if granted a warrant) but not computerized ones.

AMITAI ETZIONI, *THE LIMITS OF PRIVACY* 91–92 (1999); see also A. Michael Froomkin, *Cyberspace and Privacy: A New Legal Paradigm? The Death of Privacy?*, 52 STAN. L. REV. 1461, 1484, 1487 (2000); A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PENN. L. REV. 709 (1995); Eben Moglen, *So Much for Savages: Navajo 1, Government 0 in Final Moments of Play*, 3 N.Y.U. J. LEGIS. & PUB. POL'Y 51 (1999); Maricela Segura, *Is Carnivore Devouring Your Privacy*, 75 S. CAL. L. REV. 231 (2002); *Question and Answer Session Following Panel I*, 3 N.Y.U. J. LEGIS. & PUB. POL'Y 21 (1999) (statement of Professor Ronald K. Noble, New York University School of Law);

What is the problem if law enforcement is only seeking the same kinds of opportunities that they have currently — that is, they do not want the law to give them any more rights than they currently have, they just do not want technology to defeat what the law permits — what is wrong with that?

people use to communicate personal information — namely telephones and other electronic devices.¹¹³ As the Supreme Court recently explained:

Over 30 years ago, with Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Congress recognized that the “[t]remendous scientific and technological developments that have taken place in the last century have made possible today the widespread use and abuse of electronic surveillance techniques. As a result of these developments, privacy of communication is seriously jeopardized by these techniques of surveillance No longer is it possible, in short, for each man to retreat into his home and be left alone. Every spoken word relating to each man’s personal, marital, religious, political, or commercial concerns can be intercepted by an unseen auditor and turned against the speaker to the auditor’s advantage.”¹¹⁴

The wiretap laws generally prohibit third parties from intercepting communications. They permit police interception of communications, but only after the police satisfy requirements more demanding than those applicable to intrusions.¹¹⁵ By conferring such protection, Congress sought to restore citizens’ confidence in telephonic (and other) communications by reestablishing the integrity of communications over telecommunications devices.¹¹⁶

Wiretap laws have generally proven effective in preventing nongovernmental third parties from intercepting covered communications.¹¹⁷ However, the Supreme

¹¹³ The Electronic Communications Privacy Act of 1986, the successor to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, categorizes communications as oral, wire, and electronic. Oral communications are defined as “oral communication uttered by a person” and generally involve people within speaking distance communicating without the use of a telephone or other communications equipment. 18 U.S.C. § 2510(2) (2000). Wire communications are defined as “*aural transfer[s]* made in whole or in part through the use of facilities for transmission . . . by . . . wire, cable, or other like connection,” *i.e.*, communications using telephone lines and the equivalent. 18 U.S.C. § 2510(1). Electronic communications are defined as “any transfer of signs, signals, data, writings, images, sound data or intelligence” transmitted in whole or in part by “wire, radio, electromagnetic, photoelectric, or photooptical system” that falls outside the definitions of oral or wire communications. 18 U.S.C. § 2510(12). For example, faxes and e-mails would be categorized as electronic communications. *See generally* LAFAYE ET AL., *supra* note 20, at 269–72; FISHMAN & MCKENNA, *supra* note 100, §§ 2:8–13, 2:14–27, 3:2.

¹¹⁴ *Bartnicki v. Vopper*, 532 U.S. 514, 542–43 (2001) (quoting S. REP. NO. 1097, 90th Cong., 2d Sess. 67 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2154).

¹¹⁵ *See generally* FISHMAN & MCKENNA, *supra* note 100.

¹¹⁶ *Bartnicki*, 532 U.S. at 523, 526; *id.* at 541–42 (Rehnquist, C.J., dissenting).

¹¹⁷ ECPA allows some private third-party interception of covered communications. Employers may sometimes monitor employees’ communications, and some members of a household may monitor the communications of co-habitants. ECPA allows employers to

Court's recent decision in *Bartnicki v. Vopper*¹¹⁸ introduces a subject matter test into the wiretap law provisions regarding dissemination of illegally-wiretapped conversations.¹¹⁹ In *Bartnicki*, a disc jockey played over the air a tape recording of a cell phone conversation between two union leaders. The unknown person who had illegally recorded the call had delivered a copy of the tape to the disc jockey.¹²⁰ The Electronic Communications Privacy Act ("ECPA") prohibits anyone from divulging a conversation if he or she has reason to believe that the conversation was intercepted in violation of ECPA, regardless of whether or not such person participated in the illegal interception. The Court held that the First Amendment precluded punishing a person not implicated in the illegal interception from divulging the contents of illegally wiretapped conversations that involved matters of public importance.

Perhaps the most disturbing aspect of the Court's opinion is the Court's comment that the disc jockey could publish the information derived from the illegal interception of a wire communication because the statements made in the course of the private call would have been newsworthy had they been made in a public setting.¹²¹ In effect, the majority treated the means of communication, namely a private phone conversation rather than a public statement, as irrelevant to the speakers' legitimate expectations of privacy. The Court did so even though the wiretap laws it was addressing specifically focused privacy protection on the means of communication (not subject matter considerations).

In criminal cases, courts have split on whether law enforcement can use the

monitor employee conversations by using commercially available telephone equipment in the ordinary course of the employer's business. 18 U.S.C. §§ 2510(4), 2510(5)(a)(I); *see also* FISHMAN & MCKENNA, *supra* note 100, §§ 7:3–11. Citing the Omnibus Crime Control Act's legislative history, some courts have engrafted a "marital home" exception upon the statutory text that allows some members of a household to surreptitiously listen in on the conversations of others. *See, e.g.,* *Simpson v. Simpson*, 490 F.2d 803 (5th Cir. 1974); FISHMAN & MCKENNA, *supra* note 100, §§ 7:12–18.

¹¹⁸ 532 U.S. 514 (2001).

¹¹⁹ *Id.* at 534–35. Journalists who have no role in the illegal interception of oral, electronic, or wire communication cannot be liable for disclosing information obtained from the illegal interception, even if they had reason to know the interception was illegal, if the subject matter of the conversation was a matter of public concern.

¹²⁰ The illegally intercepted conversation between a local union head and the union's chief negotiator concerned contract negotiation with the local school board. During the call, the union president asserted that if the school board did not meet the union's demands (or at least show more flexibility), "we're gonna have to go to their, their homes To blow off their front porches, we'll have to do some work on some of those guys." *Id.* at 518–19 (omission in original). There is no indication that any action was taken consistent with those assertions.

¹²¹ *Bartnicki*, 532 U.S. at 525 ("If the statements about the labor negotiations had been made in a public arena — during a bargaining session, for example — they would have been newsworthy. That would also be true if a third party had inadvertently overheard Bartnicki making the same statements to Kane when the two thought they were alone.").

contents of communications illegally intercepted by others.¹²² *Bartnicki* will strengthen the argument for police use of illegally wiretapped conversations. Indeed, *Bartnicki* itself, albeit in a different context, declares criminal activity itself a matter of public interest.

Some means of communication are particularly disfavored, in large part due to anomalies in constitutional doctrine. Writings, for instance, leave a physical presence which makes them subject to subpoenas calling for their production. The similarity between writing and testimony was a foundation of the Court's now defunct opinion in *Boyd v. United States*,¹²³ In *Boyd* the Court held that the Fifth Amendment precluded subpoenas compelling production of incriminating written records,¹²⁴ equating compelled production of incriminating writings with compelled production of testimony.¹²⁵

But consent also defeats means-of-communication privacy protections, at least when it is law enforcement agents or their collaborators who obtain the consent.¹²⁶ The power of private undercover investigators to rely on fraudulently obtained consent as a defense against privacy claims is unclear.¹²⁷

¹²² Matt Greenberg, *Law Enforcement Officer With Clean Hands May Not Make Investigative Use of Wiretap That Was Illegally Acquired by a Third Party*: *Berry v. Funk*, 146 F.3d 1003 (D.C. Cir. 1998), 68 U. CIN. L. REV. 463 (2000); see also *United States v. Smith*, 155 F.3d 1051 (9th Cir. 1998); *United States v. Murdock*, 63 F.3d 1391 (6th Cir. 1995); *United States v. Vest*, 813 F.2d 477 (1st Cir. 1987); *Spetalieri v. Kavanaugh*, 36 F. Supp. 2d 93 (N.D.N.Y. 1998).

¹²³ 116 U.S. 616, 637 (1886).

¹²⁴ *Stuntz*, *supra* note 7, at 1041–42; see also *Boyd*, 116 U.S. at 630 (holding that “any forcible and compulsory extortion of a man’s own testimony or of his private papers to be used as evidence to convict him of crime” is barred by the Fifth Amendment).

¹²⁵ The current distinction between compelled production of documents and compelled testimony could, alternatively, reflect an analysis focused on the means of intrusion. Perhaps subpoenas cause less alarm than searches because subpoenas have a passive quality. The citizens whose papers are subpoenaed identify the relevant papers and produce them. Contrastingly, during searches, law enforcement officers peruse large amounts of material, much of which may be irrelevant, to identify the material relevant to the investigation. See *Okla. Press Publ’g Co. v. Walling*, 327 U.S. 186, 194–96 (1946); *PIERCE ET AL.*, *supra* note 19, § 8.2, at 408–09 (3d ed. 1999).

¹²⁶ See *United States v. White*, 401 U.S. 745 (1971); *Hoffa v. United States*, 385 U.S. 293 (1966); *Lopez v. United States*, 373 U.S. 427 (1963); *Lee v. United States*, 343 U.S. 747 (1952); *Food Lion, Inc. v. Capital Cities/ABC, Inc.*, 194 F.3d 505 (4th Cir. 1999); *Dietemann v. Time, Inc.*, 449 F.2d 245 (9th Cir. 1971).

¹²⁷ In the civil context, means-of-communications protection can also be subverted by property rights. For example, the owner of an e-mail network, who may be a large employer, has a right to monitor messages transmitted over its system. 18 U.S.C. § 2701(c) (2000); see also 18 U.S.C. § 2510(5) (providing ordinary business exception to wiretap laws); *Epps v. St. Mary’s Hosp.*, 802 F.2d 412, 416–17 (11th Cir. 1986); *James v. Newspaper Agency Corp.*, 591 F.2d 579, 581 (10th Cir. 1979); *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996); *TURKINGTON & ALLEN*, *supra* note 108, at 267; cf. *Deal v. Spears*, 980 F.2d 1153,

Dealing with undercover techniques and deceptive acquisition of consent by distinguishing among means of communication has little merit. No particular means of communication seems more intimate than others. At least there is too little difference to make worthwhile differentiating the methods of regulation based on the means of communication involved.¹²⁸

In short, laws sometimes protect privacy by ensuring that communications can remain confidential.

C. The Means of Intrusion as a Mode of Privacy

Occasionally, privacy protection is focused on controlling particular means of intrusion. For example, electronic recording has received special attention.¹²⁹ In civil, and sometimes even criminal, contexts, courts consider recording a conversation more problematic than repeating it. Take the case of *Dietemann v.*

1157 (8th Cir. 1992) (stating that consent may be implied); *United States v. Harpel*, 493 F.2d 346, 351 (10th Cir. 1974) (stating that private telephone conversations are held to a higher level of scrutiny).

Elements of location and interpersonal relationships also have a factor in considering the sanctity of telephone communication, thus courts have created a domestic exception to the wiretap laws. *TURKINGTON & ALLEN*, *supra* note 108, at 280-87.

¹²⁸ Means can also be certain types of items. For instance, items particularly affiliated with internal thought might enjoy heightened protection. Indeed, this seems to have been a major concern expressed by Warren and Brandeis in their seminal article. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) ("The common law secures to each individual the right of determining ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others"); *see also* *Olmstead v. United States*, 277 U.S. 438, 478 (Brandeis, J., dissenting):

The makers of our Constitution . . . recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations.

For example, diaries may receive greater protection than other documentary records. *See United States v. Doe*, 465 U.S. 605, 619 n.2 (1984) (Marshall, J., concurring) ("[T]he documents at stake here are business records which implicate a lesser degree of concern for privacy interests than, for example, personal diaries."); *Couch v. United States*, 409 U.S. 322, 350 (1972) (Marshall, J., dissenting) ("Diaries and personal letters that record only their author's personal thoughts lie at the heart of our sense of privacy."). Public library records, which record the materials one reads by recording the material checked out might also be given heightened protection. *E.g.*, CONN. GEN. STAT. ANN. § 11-25 (West 1986); N.J. STAT. ANN. § 18A:73-43.2 (West 1989); N.Y. C.P.L.R. 4509 (McKinney 1989); *see also* Ulrika Ault, *The FBI's Library Awareness Program: Is Big Brother Reading Over Your Shoulder?*, 65 N.Y.U. L. REV. 1532 (1990).

¹²⁹ *See Zimmerman, supra* note 30, at 1208-18.

Time, Inc.,¹³⁰ in which a homeowner who offered clay, mineral and herbal remedies for various medical conditions sued journalists who entered his home under false pretenses, allegedly seeking treatment. During their visit the journalists had used hidden audio and video recording equipment to document their interaction with Dietemann. The Court found that the journalists had wrongfully invaded Dietemann's privacy, but not because the reporters' had been unfaithful confidants (*i.e.*, false friends), who had willingly disclosed the observations he made while in Dietemann's home under false pretenses. Members of society must accept such a risk. But the court distinguished the risk of being electronically recorded within one's home from the risk posed by tattling "false friends," and concluded that members of society should not have to assume such a risk.

In contrast, the United States Supreme Court, in applying the Fourth Amendment to criminal investigations, has equated electronically recorded undercover conversations with investigative targets and undercover efforts lacking such electronic monitoring. Some state supreme courts have adopted a contrary view, holding that even law enforcement undercover operations using electronic monitoring must be treated more seriously than those that do not.¹³¹

At first glance, as the Supreme Court suggested in *United States v. Lopez* and *United States v. White*,¹³² prohibiting electronic recording merely enables speakers to "plausibly deny" statements that they did indeed make.¹³³ As the *Lopez* majority opined:

Stripped to its essentials, petitioner's argument amounts to saying that he has a constitutional right to rely on possible flaws in the agent's memory, or to challenge the agent's credibility without being beset by corroborating evidence that is not susceptible of impeachment. For no other argument can justify excluding an accurate version of a conversation that the agent could testify to from memory.¹³⁴

A plea for legal protection to facilitate dissimulation is difficult to justify, especially in the context of criminal or regulatory investigations. But perhaps alternative explanations justify treating recordings and replaying conversations differently from repeating conversations without using recording equipment. Use of recording

¹³⁰ See *Dietemann v. Time, Inc.*, 449 F.2d 245, 249 (9th Cir. 1971).

¹³¹ *State v. Glass*, 583 P.2d 872, 881 (Alaska 1978); *State v. Hayes*, 752 A.2d 16 (Vt. 2000); *State v. Blow*, 602 A.2d 556 (Vt. 1991).

¹³² *White v. United States*, 401 U.S. 745 (1971).

¹³³ *Lopez v. United States*, 373 U.S. 427, 439 (1963); see also *White*, 401 U.S. at 753 ("[W]e are not prepared to hold that a defendant who has no constitutional right to exclude the informer's unaided testimony nevertheless has a Fourth Amendment privilege against a more accurate version of the events in question.").

¹³⁴ *Lopez*, 373 U.S. at 439.

equipment may cause heightened concern because recordings capture details of a speaker's facial expressions or intonation which renditions of conversations from memory do not. However, such an explanation warrants some skepticism. Some who possess both an excellent memory and a facility for imitation can surely report a conversation by mimicking the original speaker, yet surely their doing so would not be considered especially problematic.

A sound, but not especially rigorous explanation for the greater seriousness with which we treat recording conversations might be grounded in the intuition that the impermanent differs from the permanent.¹³⁵ Before going on the record (*i.e.*, setting forth thoughts in permanent form), people should know they are on the record and have an opportunity to craft their words precisely. Such a principle restores a rough equality between speakers and recipients — speakers will have an opportunity to put substantial effort into crafting their speech, just as recipients will have an opportunity to devote substantial attention to analyzing it.

Ultimately, however, this interest, while substantial, might not outweigh society's interest in the prosecution of crime or the effective regulation of conduct legitimately subject to government constraint. The interest in allowing speakers to craft their words precisely before those words take permanent form may, however, outweigh the interests furthered by allowing private citizens to surreptitiously record conversations in which they participate. Such interests include ensuring that the populace learns information of public importance necessary to exercise the right of self-government and ensuring that individuals have the information they need to exercise autonomy.¹³⁶ Because First Amendment doctrine distinguishes speech from conduct, making conduct subject to greater regulation,¹³⁷ legislators can impose criminal and civil liability upon electronic recording of conversations even if the act of recording is performed to obtain information of genuine public concern.¹³⁸

¹³⁵ *White*, 401 U.S. at 787 (Harlan, J., dissenting) ("Authority is hardly required to support the proposition that words would be measured a good deal more carefully and communication inhibited if one suspected that his conversation were being transmitted and transcribed."). Justice Harlan observed:

Much off-hand exchange is easily forgotten and one may count on the obscurity of his remarks, protected by the very fact of a limited audience, and the likelihood that the listener will either overlook or forget what is said, as well as the listener's inability to reformulate a conversation without having to contend with a documented record. All these values are sacrificed by a rule of law that permits official monitoring of private discourse limited only by the need to locate a willing assistant.

Id. at 787–89 (Harlan, J., dissenting) (footnote omitted).

¹³⁶ *Bell*, *supra* note 11, at 778 n.146.

¹³⁷ *Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 253 (2002); *Bartnicki v. Vopper*, 532 U.S. 514, 535 (2001).

¹³⁸ Computerization is also especially problematic. Computerization of records removes

Indeed, an appreciation that the means of intrusion can raise special privacy concerns might address some of the criticisms leveled against the Court's location-focused Fourth Amendment doctrine. Invasion of privacy may, ultimately, often merely consist of focusing undue attention upon others, as Professor Jeffrey Rosen has recently suggested.¹³⁹ As Fourth Amendment law has developed, law enforcement officers can focus on individuals in "public" spaces for as long, and in as much detail, as they desire. The courts could embrace a slightly different Fourth Amendment approach. They could continue to rule that law enforcement officials need not avert their eyes from matters they and members of the public would naturally observe momentarily as they go about their business. However, government officials must satisfy the warrant and probable cause requirements (or identify appropriate exception) before focusing unusual attention upon such matters. Differences in the degree of attention directed at people or property in public spaces (or observable from public spaces) do not alter a location-based analysis, but may well alter an analysis focused on the means of intruding upon others. The difference in the amount of attention given from a public place is not a location-based difference, but a difference in the means of intrusion.

Under the foregoing analysis, Fourth Amendment cases involving aerial surveillance might be resolved differently. The Court has held that because aircraft operate in public space — namely the airways controlled by the Federal Aviation Administration (the "FAA") — and because any passenger may freely look into an enclosed backyard as he travels past it, law enforcement officers may photograph enclosed backyards (using detail-enlarging enhancements if necessary) or hover

the "practical obscurity," *U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 762 (1989), of records that are "available" but difficult to acquire and compile. Thus, Congress has imposed special restrictions on federal agencies' use of computer matching. Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a(o) (2000). Similarly the federal and state courts have begun to address concerns about computerization of court records. Such computerization surely has more serious privacy implications than mere maintenance of the court records themselves. Kate Marquess, *Open Court?: As Courthouses Rush to Put Filing Online, Easy Access to Legal Documents Has Many Worrying About Privacy Rights*, A.B.A.J., Apr. 2002, at 54; see also JUDICIAL CONFERENCE COMM. ON COURT ADMIN. & CASE MGMT. REPORT ON PRIVACY AND PUBLIC ACCESS TO ELECTRONIC CASE FILES (2001), available at <http://www.privacy.uscourts.gov/Policy.htm>; MARTHA WADE STEKETEE & ALAN CARLSON, NAT'L CTR. FOR STATE COURTS & JUSTICE MGMT. INST., *DEVELOPING CCJ/COSCA GUIDELINES FOR PUBLIC ACCESS TO COURT RECORDS: A NATIONAL PROJECT TO ASSIST STATE COURTS* (2002), available at <http://www.courtaccess.org/modelpolicy/18Oct2002FinalReport.pdf>. In the nongovernmental realm, Amatai Etzione has discussed the implications of computerization of medical records for medical privacy. ETZIONE, *supra* note 112, at 142–43.

¹³⁹ JEFFREY ROSEN, *THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA* 16–18 (2001) (discussing "civil inattention" — an expectation of a zone of privacy among strangers).

over such yards for extended periods, examining their contents or any activities occurring therein.¹⁴⁰ By focusing on the nature of the intrusion, and in particular the offense to privacy that occurs when strangers pay undue attention to each other, we might distinguish the conduct of an airplane passenger or law enforcement officer who happens to observe incriminating activity as she goes about her business and the law enforcement officer, journalist, or private citizen who hovers over the same yard and concentrates on the activity occurring in that yard.

Undercover activity itself could be subjected to regulation as a particularly problematic means of intruding into privacy. Government use of deception is inherently problematic.¹⁴¹ Moreover, such deception can produce several related problems. Undercover operations may lead investigatory targets to commit criminal acts they would otherwise never have committed, due to the lack of opportunity.¹⁴² Public knowledge of deceptive tactics may also enable some miscreants to engage in criminal acts by posing as undercover law enforcement officers.¹⁴³ And indeed, some confidential informants used by law enforcement in undercover settings engage in independent crimes for their own benefit while acting as confidential informants. For example, Mark A. Whiteacre, an Archer Daniels Midland Co. executive, embezzled millions of dollars while operating as a confidential informant assisting the FBI's investigation of the company for antitrust violations.¹⁴⁴ Even non-targets whom the government must deceive in the course of an undercover investigation may suffer loss. For instance, the Fifth Circuit recently considered a damages action brought by an executive whose career had suffered when he left a legitimate business to join a business established by the FBI as a part of a "sting"

¹⁴⁰ See *California v. Ciraolo*, 476 U.S. 207, 215 n.3 (1986); FISHMAN & MCKENNA, *supra* note 100, § 29:16.

¹⁴¹ See generally SISSELA BOK, *LYING: MORAL CHOICE IN PUBLIC AND PRIVATE LIFE* 174–191 (1978).

¹⁴² This problem is addressed by the entrapment defense, see *Russell*, 411 U.S. at 435–36; LAFAVE ET AL., *supra* note 20, §§ 5.1–5.2; LAFAVE & SCOTT, *supra* note 39, § 5.2; MARX, *supra* note 8, at 188–90, although even the entrapment defense deals only with the lack of desire to commit the crime rather than the lack of resources to commit it, though courts sometimes disagree about how to deal with situations in which law enforcement officials provide essential help to commit the crime. See generally PAUL MARCUS, *THE ENTRAPMENT DEFENSE* (2d ed. 1995).

¹⁴³ MARX, *supra* note 8, at 146, 176.

¹⁴⁴ *United States v. Andreas*, 216 F.3d 645, 654–55 (2000); see also MARX, *supra* note 8, at 144–45; Amanda J. Schreiber, *Dealing with the Devil: An Examination of the FBI's Troubled Relationship with Its Confidential Informants*, 34 COLUM. J.L. & SOC. PROBS. 301 (2001). The FBI has recently adopted new guidelines on the handling of confidential informants. THE ATTORNEY GENERAL'S GUIDELINES ON FEDERAL BUREAU OF INVESTIGATION UNDERCOVER OPERATIONS 7 (2002) [hereinafter FBI GUIDELINES], available at <http://www.usdoj.gov/olp/fbiundercover.pdf>.

operation.¹⁴⁵

Not only is government deception inherently problematic, but undercover investigations often take on the quality of a "general search,"¹⁴⁶ i.e., an unfocused search to uncover possible criminality not directed toward discovering any particular item or person. The Framers of the Bill of Rights considered general searches particularly abhorrent.¹⁴⁷ Undercover techniques allow agents and confidential informants to gather large amounts of information about the investigative target and his activities, much of which has no relevance to the crime agents suspect the target of committing. Indeed, such techniques allow law enforcement to simply test the integrity of the target without having any reason to suspect the individual of wrongdoing.

However, courts have justifiably exhibited a reluctance to place limits on undercover work as a mode of investigation. Such investigations have proven essential and effective in a variety of circumstances, as the Supreme Court has noted.¹⁴⁸ Moreover, undercover operations are not an inherent affront to privacy. For example, posing as a customer or as a potential home buyer should not be considered an invasion of the retailer's or realtor's privacy (even though such conduct is deceptive). Nor do undercover operations inherently possess the quality of a general search.

Some undercover operations are quite narrowly focused, and the targets largely select themselves. For example, government-operated fake fencing operations or decoy prostitutes will probably ensnare only those interested in engaging in illegal conduct, and will largely uncover information relevant to potential criminal prosecution.¹⁴⁹

In short, a focus on the means of intrusion can sometimes produce a more subtle

¹⁴⁵ *Brown v. Nationsbank Corp.*, 188 F.3d 579 (5th Cir. 1999).

¹⁴⁶ E.g., Tracey Maclin, *Informants and the Fourth Amendment: a Reconsideration*, 74 WASH. U.L.Q. 573, 578–85 (1996); Slobogin, *supra* note 94, at 807.

¹⁴⁷ See *Payton v. New York*, 445 U.S. 573, 583 n.21 (1980); *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971); William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning 1494–1508* (1990) (unpublished Ph.D. dissertation, Claremont Graduate School) (on file with the University of Michigan Dissertation Information Service).

¹⁴⁸ See *United States v. Russell*, 411 U.S. 423, 435–36 (1973) (asserting that sometimes "deceit is the only practicable law enforcement technique available"); *Hoffa v. United States*, 385 U.S. 293, 311 (1966) ("Courts have countenanced the use of informers from time immemorial; in cases of conspiracy, or in other cases when the crime consists of preparing for another crime, it is usually necessary to rely upon them or upon accomplices because the criminals will almost certainly proceed covertly.") (quoting *United States v. Dennis*, 183 F.2d 201, 224 (2d Cir. 1950) (Learned Hand, J.), *aff'd*, 341 U.S. 494 (1951)); *Lewis v. United States*, 385 U.S. 206, 210 (1966); *Sorrells v. United States*, 287 U.S. 435, 441–42 (1932); *Andrews v. United States*, 162 U.S. 420, 423 (1896); *Grimm v. United States*, 156 U.S. 604, 610 (1895).

¹⁴⁹ MARX, *supra* note 8, at 71–72.

and realistic analysis of privacy issues than that derived from either the location-based or means-of-communication-based perspectives outlined previously.

D. Subject Matter as a Mode of Privacy

Sometimes the protection offered by privacy law depends on the subject matter at issue. Some information may qualify as private, and thus may not be subject to public discussion absent the consent of the person to whom the information pertains. Such a subject matter approach could take precedence over a competing approach, such as the traditional location-focused mode of analysis. In a media case, *Daily Times Democrat v. Graham*,¹⁵⁰ the Alabama Supreme Court considered whether to hold a photojournalist liable for publishing his photograph of a woman whose dress had been blown upward unexpectedly by an air vent, revealing her undergarments. The woman brought a cause of action for publication of private facts.

At the time the picture was taken, both the woman and the photographer were in a public place — a county fair. A location-based analysis would have suggested that the *Daily Times Democrat* could publish the picture. Instead, the Court focused on the subject matter of the picture, which it characterized as involving indecent exposure. The Court thus held wrongful the taking and distribution of photographs showing a person's underwear in circumstances where the subject neither intentionally exposed her underwear nor consented to the publication of the photograph.¹⁵¹ Note, however, that the Court could have reached the opposite result using a subject-matter-based analysis, the photograph captures an unusual event that might remind readers of a popular image of then-widely acclaimed movie star Marilyn Monroe.¹⁵²

A subject-matter approach could encompass the acquisition of information, as well as public discussion of information.¹⁵³ Thus, it is inappropriate to ask strangers

¹⁵⁰ 162 So.2d 474 (Ala. 1964).

¹⁵¹ The Court could have focused on the means of intrusion. It might have found tortious either intentionally photographing a person in such a predicament or showing such a picture to others, but allowed an observer to describe the event. The permanence of the photograph could have been identified as the core privacy problem. Such an approach would have protected Graham, the subject of the photograph, had the photographer merely retained the photograph and shown it to a few friends rather than publishing the photograph in a newspaper.

¹⁵² *THE SEVEN YEAR ITCH* (20th Century Fox 1955) (scene in which Marilyn Monroe's dress blown upward as she stood over an air vent).

¹⁵³ The constitutional law doctrine permitting welfare inspections of recipients' homes without individualized suspicion or a warrant may be illustrative. In that context, which involves information acquisition, a subject-matter analysis trumps a location-based analysis. In *Wyman v. James*, 400 U.S. 309 (1971), the Supreme Court confronted a Fourth Amendment challenge to social service agency caseworkers' inspections of recipients homes

about their salary, the amount of money in their bank account, or the type of undergarments they wear. The notoriety of the "boxers or brief" question asked of President Clinton during a 1994 appearance on MTV illustrates the point.¹⁵⁴

Of course, with regard to the acquisition of information, society need only address coercive requests for information (such as "no information, no job" or "no information, no credit").¹⁵⁵ Not only can individuals otherwise control their own disclosure of personal information (assuming they have dominion over some physical location that affords privacy and can control the repetition of the information they entrust to others), the ability to selectively provide such information is a necessary element of intimacy.¹⁵⁶ We may define our circle of friends by our willingness to share private information about ourselves with them. Thus, the subject matter mode most often addresses dissemination of information,

pursuant to the Aid to Families with Dependent Children ("AFDC") program. Though the home, as a location, receives paramount privacy protection, and citizens generally have a reasonable expectation of privacy in their dwellings, the Court found that state officials, in making home inspections, had breached no expectation of privacy of the aid recipients. Thus, such home inspections without individualized suspicion and a warrant did not contravene the Fourth Amendment.

One can explain the Court's rejection of the location-based analysis by viewing the case as turning on consent. The recipient had the right to exclude caseworkers, which she waived by seeking to participate in the AFDC program. *Id.* at 317-18, 321-22. However, one might also view the case as holding that conditions in the recipient's home became a matter of public concern once she began receiving aid under the AFDC program. *Id.* at 318-19. This subject-matter aspect of the Court's analysis suggests that aid recipients have no right of privacy in the condition of their homes given the relevance of those conditions to both their continued eligibility for the AFDC program and an assessment of the aid's efficacy.

The *Wyman* Court also relied, in part, on a means of intrusion approach to uphold the home inspections. *Id.* at 320-21 ("The means employed by [the state agency] are significant."). The Court noted that authorities engaged in no snooping, provided the recipient advanced written notice of the inspection, and used no deception in conducting the home inspection — in short, the means of intrusion were "gentle." *Id.* at 319-21. Analysis of privacy expectations based on the subject matter and means of intrusion were simply considered as more relevant than the location of the intrusion, the aspect of the case the dissenters emphasized. *Id.* at 327-38, 332-33, 334-35 (Douglas, J., dissenting); *id.* at 338-47 (Brennan, J., dissenting).

¹⁵⁴ See, e.g., Brian Balogh, *An Evolving Presidency*, L.A. TIMES, Aug. 2, 1998, at M1; Howard Witt, *Powell on MTV Show, Urges Condom Use to Prevent AIDS*, CHI. TRIB., Feb. 15, 2002. For an account of Clinton's MTV appearance, see *Clinton Gives Revealing Answers to MTV Crowd*, CHI. TRIB., Apr. 26, 1994, at 3.

¹⁵⁵ See *infra* note 172 (concerning requests for HIV status or genetic information for purposes of insurance).

¹⁵⁶ Charles Fried, *Privacy*, 77 YALE L.J. 475, 484 (1968) (noting that love and friendship require different levels of disclosure; without the ability to differentiate the level of disclosure of facts about oneself, there can be no love or respect); see also Bell, *supra* note 11, at 770 & n.109.

rather than access.

The subject matter mode of privacy has some relevance to criminal investigation because some subject matter constraints are imposed on investigations. However, subject matter limitations serve as only the most mild constraint on criminal investigations. As we shall see, the constraints are largely those of relevance. Given the growing scope of criminal liability, a relevancy standard offers little privacy protection.¹⁵⁷

The subject matter constraints on criminal investigation relate largely to relevance and law enforcement purpose. Thus, subpoenas may only request materials relevant to the criminal investigation.¹⁵⁸ Courts do, however, view relevance broadly, and thus government investigators can generally satisfy the relevance standard quite easily.¹⁵⁹ Searches and seizures must serve a law enforcement purpose.¹⁶⁰ Police officers have been found to unlawfully invade a crime victim's privacy by photographing her nude body even though the photographs could not further their efforts to apprehend the perpetrator.¹⁶¹ Law enforcement officers have also been found potentially liable for allowing journalists

¹⁵⁷ Some scholars have noted that the expansion of criminal liability makes more information relevant to criminal investigations. See, e.g., Sherry F. Colb, *The Qualitative Dimension of Fourth Amendment "Reasonableness,"* 98 COLUM. L. REV. 1642, 1651 (1998) (observing that the pervasiveness of traffic regulation gives police officers the discretion to stop virtually any car, for some traffic infraction, to investigate suspicions that the driver is involved in some criminal activity); William J. Stuntz, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 864 (2001) [hereinafter Stuntz, *Transsubstantive Fourth Amendment*]; Stuntz, *supra* note 7, at 1026; cf. ROSEN, *supra* note 139, at 79, 81, 84, 87-88 (suggesting that the expansion of conduct constituting employment discrimination has led to a reduction in employees' privacy). William Stuntz suggests that the politics of criminal law create systemic pressure to increase the number of crimes (though perhaps the pressure merely encourages an expansion of the number of ways particular conduct can be characterized as criminal). William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505 (2001). At the same time, the Supreme Court has rarely subjected the substantive scope of criminal liability to judicial review. See Sherry F. Colb, *Freedom From Incarceration: Why is this Right Different from All Other Rights*, 69 N.Y.U. L. REV. 781, 790-94 (1994).

¹⁵⁸ *United States v. R. Enters.*, 498 U.S. 292, 301 (1991) ("Where . . . a subpoena is challenged on relevancy grounds, the motion to quash must be denied unless the district court determines that there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation."); *Okla. Press Publ'g Co. v. Walling*, 327 U.S. 186, 209 (1946) ("The requirement of 'probable cause, . . . ' applicable in the case of a warrant, is satisfied in that of an order for production by the court's determination that the investigation is authorized by Congress, is for a purpose Congress can order, and the documents sought are relevant to the inquiry.").

¹⁵⁹ PIERCE ET AL., *supra* note 19, at 412 n.44.

¹⁶⁰ *Wilson v. Layne*, 526 U.S. 603, 611 (1999).

¹⁶¹ *York v. Story*, 324 F.2d 450 (9th Cir. 1963).

to accompany them on searches of private residences.¹⁶² In each case, the court held that the police actions constituted a wrongful invasion of plaintiff's privacy because the challenged act lacked a law enforcement purpose.¹⁶³

However, judicial acceptance of government intrusion in the course of acquiring information may be premised, in part, on government officials' limited interest in broad dissemination of much of the "private" information it obtains.¹⁶⁴ There are relatively few formal limits on the dissemination of information by law enforcement or regulators.¹⁶⁵ Law enforcement dissemination of information is often relatively constrained. Generally, law enforcement officials do not divulge information except to prosecute an individual or to alert the public to some illegal act or course of conduct. Administrative agencies, publicize a wider range of information — they certainly do not limit themselves to information related to criminal prosecutions.¹⁶⁶

¹⁶² *Wilson v. Layne*, 525 U.S. 603 (1999).

¹⁶³ *Id.* at 609, 611; *York*, 324 F.2d at 455; *see also* *Lauro v. Charles*, 219 F.3d 202, 213 (2d Cir. 2000) (holding staged "perp walk" unconstitutional in certain circumstances because it serves no law enforcement purpose).

¹⁶⁴ *See, e.g., Whalen v. Roe*, 429 U.S. 589 (1977) (holding that dissemination of information on patients prescribed certain drugs was not an invasion of privacy); *TURKINGTON & ALLEN*, *supra* note 108, at 67–68 (arguing that dissemination among state employees is not important); *see also* *Wilkinson v. Times Mirror Corp.*, 264 Cal. Rptr. 194 (Cal. Ct. App. 1989); *ROSEN*, *supra* note 139, at 42; *TURKINGTON & ALLEN*, *supra* note 108, at 177. *See generally* Seth F. Kreimer, *Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1 (1991); Stuntz, *supra* note 7.

¹⁶⁵ Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49, 51–53, 63–92 (1995) (suggesting that Fourth Amendment reasonableness extends to law enforcement publication of information).

One notable restraint on law enforcement officials is grand jury secrecy. *See* FED. R. CRIM. P. 6(e)(2); *LAFAVE ET AL.*, *supra* note 20, § 8.3(f), § 8.5 ("[P]ublic disclosure of the investigation may cause irreparable harm to his reputation even though the investigation eventually reveals no basis for prosecution."); Stuntz, *Transubstantive Fourth Amendment*, *supra* note 157, at 857 (criticizing Special Prosecutor Kenneth W. Starr's handling of grand jury material during his investigation of President Clinton).

There is no constitutional limitation on the dissemination of even false information. *Paul v. Davis*, 424 U.S. 693, 701 (1976). Moreover, once the government releases of information, even by mistake, citizens have a constitutional right to further disseminate that information, regardless of the subject's privacy interest in that information. *See Florida Star v. B.J.F.*, 491 U.S. 524, 536–41 (1989). Indeed, further dissemination of information obtained from the government is protected, even when it harms the victim of a crime, as long as the information was legally acquired. *See Smith v. Daily Mail Publ'g Co.*, 443 U.S. 97, 103–04 (1979). However, the government can and sometimes does impose liability on itself for such breaches of privacy.

¹⁶⁶ *Doe v. City of New York*, 15 F.3d 264, 269 (2d Cir. 1994) (recognizing agency's need to disseminate information about litigation successes, but balancing with privacy is required); JAMES T. O'REILLY, *FEDERAL INFORMATION DISCLOSURE* § 25.01 (2d ed. 1999); ELLEN

However, even their release of information is largely related to their defined public mission.

In the private realm, both the practicalities and the law differ. The media's primary mission is information dissemination,¹⁶⁷ and media entities will not limit disclosure of criminal activity or regulatory violations simply because they will not lead to criminal prosecution or administrative actions.¹⁶⁸ Tort law recognizes a cause of action for publication of private facts. That cause of action and the location-focused intrusion into seclusion cause of action discussed previously largely provide the common-law redress for breach of informational privacy. (Other privacy torts, such as false light privacy (focusing on falsity) and appropriation of likeness (focusing commercial use of citizens' faces, bodies, and names) do not really address informational privacy.) The publication of private facts action, whose developments owes more to Warren and Brandeis' pathbreaking *Harvard Law Review* article, advocating common law protection of privacy,¹⁶⁹ than does any of the other common law privacy actions, defines privacy rights in terms of subject matter. Publication of certain facts about a person constitutes an invasion of her privacy because of the subject matter involved. Plaintiff can prevail on the claim only if the defendant publicizes a private matter in which the public has no legitimate interest. The means of acquiring the information is immaterial, making the physical location, means of communication, and means of intrusion modes of privacy analysis largely irrelevant.

The ineffectiveness of the publication of private facts action as a privacy protection illustrates the difficulty of using the subject-matter mode of analysis to protect privacy. Plaintiffs can rarely successfully pursue a publication of private facts claim, because they can rarely prove that the published information reveals nothing of legitimate public concern. Indeed, virtually any information, even that we ordinarily consider personal, can be viewed as a matter of public concern.¹⁷⁰

Much activity is regulated by the government in some manner and, therefore,

ALDERMAN & CAROLINE KENNEDY, *THE RIGHT TO PRIVACY* 144 (1995) (discussing *Doe v. Borough of Barrington*, 729 F. Supp. 376 (D.N.J. 1990)); Ernest Gellhorn, *Adverse Publicity by Administrative Agencies*, 86 HARV. L. REV. 1380, 1382-1419 (1973) (discussing agency use of publicity); Lars Noah, *Administrative Arm-Twisting in the Shadow of Congressional Delegations of Authority*, 1997 WIS. L. REV. 873, 887-91; Ralph Vartabedian & Edwin Chen, *FAA to Provide Safety Reports on the Internet*, L.A. TIMES, Jan. 30, 1997, at A1.

¹⁶⁷ Bell, *supra* note 11, at 785 n.178.

¹⁶⁸ A recent example is the playing of an undercover tape capturing Al Sharpton's reaction to a proposal that he participate in a cocaine transaction. The relevant law enforcement agency did not publicly disseminate the tape presumably because it did not show activity warranting prosecution. HBO played the tape as a part of a documentary about the figure who sought to involve Sharpton in the narcotics deal. See Glenn Thrush, *Sharpton Files \$1 Billion Suit Over HBO Drug Tape*, CHI. SUN-TIMES, July 25, 2002, at 18.

¹⁶⁹ Warren & Brandeis, *supra* note 128, at 196.

¹⁷⁰ See generally ROSEN, *supra* note 139, at 48-50; Zimmerman, *supra* note 30.

is of public concern if there is a potential crime or regulatory violation. Even currently unregulated activity can be subject to regulation. Thus even such activity may qualify as a matter of public concern, so that the public can obtain the information to consider whether the current regulatory regime needs expansion, contraction, or some other change. Public servants' participation in government makes many aspects of their lives matters of public concern.

Moreover, though the First Amendment's Free Speech Clause serves to further self-government, the legitimate interests of the public encompass more than governmental affairs. Many "public figures" who play no role in government, such as corporate executives, may more profoundly affects many people's lives than government officials do.¹⁷¹ Surely facts about society in general and societal transformations are matters of public interest, as are the ordeals that individuals must face, particularly when many members of society will have to confront similar ordeals. For example, the ways in which individuals cope with the HIV infection or AIDS, including decisions they make with regard to treatment and lifestyle, have significance for the substantial number of people who must face those same challenges and who might find comfort in knowing that they are not alone.¹⁷²

As the foregoing suggests, some very personal matters may become matters of public importance because they illustrate some broader trend. For example, in *Haynes v. Alfred A. Knopf, Inc.*,¹⁷³ very personal information regarding the relationship between two ordinary people, Ruby Lee Daniels and Luther Haynes, was found a matter of public interest, precluding Haynes from prevailing on his

¹⁷¹ See *Curtis Publ'g Co. v. Butts*, 388 U.S. 130, 163-65 (1967) (Warren, C.J., concurring); see also SISSELA BOK, *SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION* 257 (1982) ("[I]t has become increasingly hard to draw a clear line between government information and information about the private sector."). The recent dramatic loss in value of Enron and WorldCom stock, which jeopardized many individual retirement plans, e.g., SEN. RPT. NO. 107-222, at 4-6 (2002) (describing the Enron scandal); Jerry Knight, *WorldCom Woes Pop the Region's Telecom Bubble*, WASH. POST, July 1, 2002, at E1 (discussing WorldCom scandal); Christopher Stern, *Worldcom Fights on 2 Fronts; Investigations into Accounting Practices Compound Firm's Fiscal Troubles*, WASH. POST, July 23, 2002, at E1 (discussing WorldCom scandal), serves as a reminder of the power private individuals and entities wield.

¹⁷² Subject matter restrictions can be more effective when defined in relation to particular activities. For instance, some statutes prohibit consideration of genetic information or HIV-positive status with regard to employment decisions. Similarly, some matters may be deemed irrelevant for purposes of compiling consumer credit histories. KIM LANE SCHEPPELE, *LEGAL SECRETS: EQUALITY AND EFFICIENCY IN THE COMMON LAW* 202-03 (1988); TURKINGTON & ALLEN, *supra* note 108, at 351. Subject matter restrictions on general public discussion will likely run afoul of the First Amendment. For example, the Florida statute struck down in *Florida Star v. B.J.F.*, 491 U.S. 524 (1989), attempted to remove from public discussion particular individuals' victimization as a result of sexual assault. See *id.* at 526.

¹⁷³ 8 F.3d 1222 (7th Cir. 1993).

publication of private facts claim. Haynes had abused Daniels. By the time a book was published describing the abuse, twenty years had passed, and Haynes had remarried and become an exemplary person, even becoming Deacon of his church. However, Haynes' abuse of his prior wife illustrated a larger trend that the offending book's author had sought to describe — namely the widespread familial dysfunction attendant the migration of five million African-Americans from the rural South to the Northern cities between 1940 and 1970 (a movement termed the Great Black Migration).¹⁷⁴

As a result of the courts' frequent recognition that nominally private information can have public importance, few publication of private facts suits succeed. Indeed, the Supreme Court recognized just this sort of problem during its early efforts to craft constitutional limitations on defamation. The Court had to decide when heightened *New York Times Co. v. Sullivan*¹⁷⁵ protection would protect speakers against defamation lawsuits. In the Court's view, such protection ensured that debate on public issues would be "uninhibited, robust, and wide-open."¹⁷⁶ However, the Court refused to premise protection on the "public" nature of the issues discussed, and instead focused on the "public" nature of the allegedly defamed individual. Applying the *New York Times v. Sullivan* standard any time an allegedly defamatory statement regarded a public issue would unduly curtail defamation liability because virtually any statement could be viewed as one regarding a matter of public interest.¹⁷⁷

¹⁷⁴ See *id.* at 1232–33. In a defamation case, information about a couple's relationship and the death of their son was deemed a matter of public importance. The husband's transfer from a mental institution to a nursing home illustrated a broader trend regarding the effects of a government deinstitutionalization program, and his was a matter of public concern. The cause of his initial institutionalization (allegedly because his wife's affair with another man and their son's consequent suicide) was relevant to the story. See *Gaeta v. N.Y. News, Inc.*, 465 N.E.2d 802–06 (N.Y. 1984); see also *Huggins v. Moore*, 726 N.E.2d 456, 460–61 (N.Y. 1999) ("[O]ur cases establish that a matter may be of public concern even though it is a 'human interest' portrayal of events in the lives of persons who are not themselves public figures, so long as some theme of legitimate public concern can reasonably be drawn from their experience.").

¹⁷⁵ 376 U.S. 254 (1964).

¹⁷⁶ *Id.* at 270.

¹⁷⁷ See *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 345–46 (1974); see also *Rosenbloom v. Metromedia, Inc.*, 403 U.S. 29, 79–80 (1970) (Marshall, J., dissenting) (observing that "all human events are arguably within the area of 'public or general concern'" and noting that the newsworthiness defense to the publication of private facts common-law tort cause of action "rais[es] serious questions whether it has substantially destroyed the right of privacy as Warren and Brandeis envisioned it"); *Troman v. Wood*, 340 N.E.2d 292, 297 (Ill. 1975) ("Whether a matter is one of public interest . . . depends to some degree on whether the media themselves have chosen to make it one."); *Rouch v. Enquirer & News*, 398 N.W.2d 245, 266 & n.28 (Mich. 1986) (observing that "'public interest' is an elusive term, and may be said to include any matter reported on by the media," and quoting Theodore H. White's

In sum, subject matter approaches currently offer little protection for privacy in general and thus offers little protection against undercover operations and their consequences. Moreover, even a robust subject-matter based approach would not remedy the deceptive access undercover techniques accomplish — which often is itself an affront to privacy.

E. Confidential Relationships as a Mode of Privacy

Privacy protections could secure privacy by precluding people in whom citizens confide from divulging their confidences. For instance, society might impose upon medical personnel a duty keep confidential the information they obtain about patients in the course of rendering care. Similarly, banking records could be, and indeed are,¹⁷⁸ protected by laws prohibiting bank officials from divulging account information to government or private individuals in all but limited circumstances. The scope of such privacy rights against prospective private intruders does not turn on subject matter considerations like “relevance,” which play a central role in the subject matter mode of privacy analysis outlined above. Even if a customer’s account information has great relevance to the customer’s fitness for a political office he seeks, the bank cannot divulge the information. Conversely, if a person obtains account information without breaching the protected bank-customer relationship (by finding the depositors misplaced checkbook), he does not violate bank secrecy laws by publishing such information.¹⁷⁹ Neither, ordinarily, will the scope of legally enforceable privacy expectations associated with confidential relationships turn on issues of physical location, means of intrusion, or means of communication.¹⁸⁰

observation about “the power of the press to set the agenda of public discussion”); Harry Kalven, Jr., *Privacy in Tort Law — Were Warren and Brandeis Wrong?*, 31 *LAW & CONTEMP. PROBS.* 326, 336 (1966):

[S]urely there is force to the simple contention that whatever is in the news media is by definition newsworthy, that the press must in the nature of things be the final arbiter of newsworthiness. The cases admittedly do not go quite this far, but they go far enough to decimate the tort.

¹⁷⁸ See, e.g., *Suburban Trust Co. v. Waller*, 408 A.2d 758, 764–65 (1979).

¹⁷⁹ A separate common law cause of action for publication of private facts might lie. Such an action would probably fail if some legitimate reason for public disclosure exists, and, particularly when the depositor is a public official or public figure such a legitimate reason can likely be established.

¹⁸⁰ Granted a court may consider such issues, but probably in the context of deciding whether the information imparted from one confidant to another was ever confidential in the first place. In particular, a court may consider such factors in determining whether the confider waived their his right to confidentiality. The location of a conversation between priest and penitent might have relevance to the confidentiality of a the communication between the two. If it occurred in a public place within earshot of others, the penitent’s

American jurisdictions generally do not protect privacy by ensuring the confidentiality of information imparted in the context of a confidential relationship — that is, jurisdictions rarely focus on relationships as a critical mode of privacy protection. Formal evidentiary privileges, such as spousal, attorney-client, priest-penitent, doctor-patient, journalist-source, do, of course, protect privacy by imposing obligations of silence upon participants in those relationships. Some testimonial privileges rest, at least in part, on a constitutional basis, forming an integral part of the exercise of a particular constitutional right. The lawyer-client¹⁸¹ and priest-penitent¹⁸² privileges serve as good examples of such quasi-constitutional testimonial privileges.¹⁸³ Some privileges, like the marital communications privilege, operate bilaterally, both parties to the relationship can preclude the other from breaching their confidences. Most, however, operate unilaterally, the obligations of confidentiality run in only one direction. Evidentiary privileges associated with professional relationships are usually unilateral, only the client's confidences, not those of the professional, receive protection.¹⁸⁴

Undercover techniques could theoretically defeat these relationship-based privacy protections as they defeat location-based and means-of-communication-based privacy protections. Thus, the courts could hold that confidential informants or undercover agents who manage to convince investigative targets to reveal information by purporting to enter into a privileged or otherwise confidential

statements to the clergyman would not qualify as confidential, because others were privy to it. *See generally* JOHN W. STRONG ET AL., MCCORMICK ON EVIDENCE § 74, at 104 (4th ed. 1992) (“[M]ost modern decisions do no more than hold that a privilege will not protect communications made under circumstances in which interception was reasonably to be anticipated.”).

¹⁸¹ Ordinarily, a law enforcement agent's attendance of a meeting between attorney and client, either surreptitiously or by invocation of the government's coercive powers, would violate the Sixth Amendment right to counsel — the ability to speak with counsel confidentially constituting a crucial aspect of that right. *See, e.g.,* *Coplon v. United States*, 191 F.2d 749, 757–59 (D.C. Cir. 1951); *see also Hoffa v. United States*, 385 U.S. 293, 306–07 (1966) (assuming *Coplon* was correctly decided). *See generally* *Weatherford v. Bursey*, 429 U.S. 545, 563 (1977) (Marshall, J., dissenting) (citing lower court rulings to support the proposition that “the essence of the Sixth Amendment right is . . . privacy of communication with counsel”) (quoting *United States v. Rosner*, 485 F.2d 1213, 1224 (2d Cir. 1973)) (omission in original).

¹⁸² *See generally* Mary Harter Mitchell, *Must Clergy Tell?: Child Abuse Reporting Requirements Versus the Clergy Privilege and Free Exercise of Religion*, 71 MINN. L. REV. 723, 793–821 (1987).

¹⁸³ With respect to the provision of family planning services, the doctor-patient privilege may also have a constitutional dimension. *See Planned Parenthood v. Casey*, 505 U.S. 833, 883–84 (1992) (plurality opinion).

¹⁸⁴ The journalist-source privilege is a bit unusual. Though only the source's confidences are privileged, the journalist can interpose the privilege even if the source consents to disclosure. *See id.* § 76.2, at 110.

relationship with them, could disclose such "confidences" in seeking to enforce criminal or regulatory laws. Courts could hold that such unfortunate investigative targets lacked any legitimate expectation of privacy in the information imparted to the undercover operative.

However, in the marital context, courts held that one spouse does not lose the marital communications privilege because the other surreptitiously allows a third party to eavesdrop, even though, ordinarily, spouses lose the marital communications privilege if third parties, even eavesdroppers, are privy to the conversation.¹⁸⁵ In *State v. Lively*,¹⁸⁶ the Washington Supreme Court held that a confidential informant could not attend alcoholics/narcotics anonymous meetings to identify drug addicts who continued selling illegal drugs.¹⁸⁷ (While communications between participants in an alcoholics or narcotics anonymous program are not covered by a formal evidentiary privilege in most jurisdictions,¹⁸⁸ the relationship between the participants is a confidential one.) Except in the most critical circumstances, courts may well prohibit undercover operatives from breaching such privileged relationships.¹⁸⁹

Many observers argue that law enforcement officers should be precluded from assuming roles that require them to enter into confidential relationships with

¹⁸⁵ See *United States v. Neal*, 532 F. Supp. 942, 947-49 (D. Colo. 1982); *People v. Dubanowski*, 394 N.E.2d 605, 606-07 (Ill. App. Ct. 1979); *Hunter v. Hunter*, 83 A.2d 401, 403-04 (Pa. Super. Ct. 1951). See generally STRONG ET AL., *supra* note 180, § 74, at 103-04 (stating that the general rule, allowing an eavesdropper to testify regarding privileged conversations, has rarely been extended to situations where a party to the conversation makes the eavesdropping possible). For an interesting incident involving one spouse surreptitiously electronically recording a conversation with the other spouse and a priest, after notifying the priest of his intentions, see Adam Liptak, *Woman Sues Priest Over Secret Tape-Recording Used in Custody Battle*, N.Y. TIMES, June 30, 2002, § 1, at 14.

¹⁸⁶ 921 P.2d 1035 (Wash. 1996).

¹⁸⁷ *Id.* at 1046, 1048-49. The case was decided on due process grounds rather than on Fourth Amendment grounds. *Id.* at 1049.

¹⁸⁸ See Thomas J. Reed, *The Futile Fifth Step: Compulsory Disclosure of Confidential Communications Among Alcoholics Anonymous Members*, 70 ST. JOHN'S L. REV. 693, 700-01 (1996).

¹⁸⁹ See *Weatherford v. Bursey*, 429 U.S. 549, 554-56 (1977). Weatherford allowed breach of attorney-client communications, but only on condition that the undercover operative who attended a privileged meeting between the target and his lawyer not report on the meeting. *Id.* Infiltration of churches has been allowed, but the contested cases do not appear to have involved revelation of protected communications between penitent and cleric. See, e.g., *United States v. Aguilar*, 883 F.2d 662, 696-705 (9th Cir. 1989) (holding that undercover agents attending and recording church meetings did not need a warrant); see also Michael F. McCarthy, Note, *Expanded Fourth Amendment Coverage: Protection from Government Infiltration of Churches*, 3 GEO. IMMIGR. L.J. 163, 170-71 (1989) (discussing Operation Sojourner, in which the INS used an informant to infiltrate a church and obtain evidence regarding alien smuggling activity).

investigative targets.¹⁹⁰ The FBI guidelines governing undercover operations, while not absolutely precluding the use of confidential relationships, require agents to meet more demanding standards to secure approval for investigations that require undercover officers to enter into a confidential relationship.¹⁹¹ Similarly, Public Health Service regulations governing the agency's drug treatment programs subject undercover operations to demanding scrutiny and preclude the use of such techniques altogether when law enforcement officials are investigating possible criminal activity by patients. Undercover techniques may be used only to investigate misdeeds of Public Health Service employees, as they are not protected by the doctor-patient privilege, but law enforcement must nevertheless satisfy the stringent Public Health Service regulations regarding undercover operations.¹⁹²

Many confidential relationships have no corresponding formal evidentiary privilege. The Supreme Court's Fourth Amendment analysis produces particularly devastating effects in such circumstances. The Court essentially grants law enforcement most-favored-nation status. It allows law enforcement to obtain any information that any private party could acquire, even a private party privy to information an individual does not reveal to the general public. Thus, in *United States v. Miller*,¹⁹³ the Court held that acquisition of banking records did not constitute a "search," explaining that such conduct breached no legitimate expectation of privacy. In the Court's view, a depositor who shared financial information with his bank could have no legitimate expectation that law enforcement officials would not thereby gain access to the information. If a person exposes information to at least one other person, he assumes the risk of exposing that information to law enforcement.¹⁹⁴

¹⁹⁰ Several commentators have suggested that courts employ a different, higher level of scrutiny in evaluating undercover operations that require the investigator to establish an intimate relationship with the target of the investigation. See e.g., Clark D. Cunningham, *A Linguistic Analysis of the Meaning of "Search" in the Fourth Amendment: A Search for Common Sense*, 73 IOWA L. REV. 541, 576-77 (1988); William J. Stuntz, *Waiving Rights in Criminal Procedure*, 75 VA. L. REV. 761, 791-94 (1989). See generally MARX, *supra* note 8, at 147-52 (discussing examples of police tactics involving the establishment of intimate relationships with suspects).

¹⁹¹ FBI GUIDELINES, *supra* note 144, at 7.

¹⁹² See 42 C.F.R. § 2.67(a), (e) (2001).

¹⁹³ 425 U.S. 435 (1976).

¹⁹⁴ Such reasoning provided the basis for the controversial Terrorism Information and Prevention System (TIPS) program proposed by the Attorney General. Law enforcement officers would encourage public utility employees to report suspicious items they observe during the course of their daily work-related routines. U.S. DEP'T OF JUSTICE, OPERATION TIPS FACT SHEET (2002), available at <http://www.policeforum.org/tips.htm>. Congress explicitly banned the program when it established the new Department of Homeland Security. Homeland Security Act of 2002, Pub. L. No. 107-296, § 880, 116 Stat. 2135, 2245. The controversy surrounding the program and Congress' swift reaction perhaps demonstrates the

Indeed, at least on a theoretical level, Supreme Court doctrine is even more troubling. In cases like *United States v. Miller*, the Court purports to apply the principle that the police are entitled to any information available to the *general public*. The logic of the Court's holdings in such cases suggests that once an individual provides information to a confidant, no legally enforceable privacy principle precludes that confidant from revealing that information to any member of the general public, a journalist, or the public at large.¹⁹⁵ Theoretically, the Court does not recognize any variation of a person's legitimate expectations of privacy based on the identity of the intruder. Accordingly, citizens have no greater expectation of privacy against the police (operating without a warrant and/or probable cause or the equivalent) than they do against journalists or any member of the public who happens to take an interest in them.

In practice, the situation is far less grim. While the Court claims to refer to general expectations of privacy in determining the scope of legitimate expectations of privacy vis-a-vis law enforcement, it really defines the general expectation of privacy vis-a-vis law enforcement based on its own balancing of the needs of law enforcement and privacy. The Court does not appear to take seriously any evidence indicating the public's actual judgment about the level of privacy expectations society should consider reasonable.¹⁹⁶ Moreover, the Court's holding that

power of the physical location mode of privacy analysis. At least as the public understood the program, most of the reporting done under the TIPS program would regard private residences, which receives the highest protection under the traditional location-based analysis.

¹⁹⁵ This approach suggests that privacy is indivisible; we have privacy against everyone, or we have it against no one. This is counter to our intuitions. See *Nat'l Treasury Employees Union v. Von Raab*, 816 F.2d 170 (5th Cir. 1987), *aff'd in part, vacated in part on other grounds*, 489 U.S. 656 (1989):

Moreover, expectations of privacy in a particular activity do not exist on an all-or-none basis. An individual, for example, may freely admit guests to his home without relinquishing the right to bar others or may open the curtains of his home to the view of unenhanced vision without consenting to the view of a telescope. Similarly, even the individual who willingly urinates in the presence of another does not "'reasonably expect to discharge urine under circumstances making . . . discover[y of] the personal physiological secrets it holds"' possible.

Id. at 175 (quoting *Capua v. City of Plainfield*, 643 F. Supp. 1507, 1513 (D.N.J. 1986) (quoting *McDonnell v. Hunter*, 612 F. Supp. 1122, 1127 (S.D. Iowa 1985), *aff'd as modified*, 809 F.2d 1302 (8th Cir. 1987)) (omission and alteration in original) (footnotes omitted); see also *Bell*, *supra* note 11, at 764 (examining the logic of this all-or-nothing reasoning).

¹⁹⁶ See Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727, 774-75 (1993). Thus, in finding no reasonable expectation of privacy in garbage placed in opaque bags for disposal, the Court disregarded a municipal ordinance that made such snooping illegal. See *California v. Greenwood*, 486 U.S. 35, 43-44 (explicitly rejecting the approach that expectations of

depositors lacked an expectation of privacy in their banking records did not leave citizens powerless to guard such records from private snoops. The Court would rarely, if ever, have occasion to apply its own Fourth Amendment anemic conception of the reasonable expectation of privacy to claims against private intruders.¹⁹⁷

Nevertheless, in the criminal context (and theoretically in the private context) the Court has held that banks can turn over banking records to snoops. Similarly, communication attributes available to the phone company could be obtained by pen registers.¹⁹⁸ The Supreme Court failed to recognize bank-customer or utility-customer relationships as confidential relationships, but they are.

A recognition that a confidential relationship may exist despite the absence of an evidentiary privilege need not require empowering individuals to preclude their confidants from testifying in all but a few limited circumstances, as is the case when an evidentiary privilege applies. Rather, the court need only recognize that a legitimate expectation of privacy exists and thus merely require law enforcement officials to either make the showing required to obtain a warrant or advance some regulatory exception to the warrant requirement before allowing government officials to breach those confidential relationships. Certainly law enforcement officers should be required to make a showing of either reasonable suspicion or probable cause before deceptively entering into a confidential relationship to obtain information from a suspect.¹⁹⁹

On the civil side, British courts have established a cause of action for breach of

privacy are determined by ordinance or other local positive law or custom). The Court could adopt a different attitude toward the public's views regarding expectations of privacy that should be considered legitimate. It could incorporate privacy rights reflected in state laws, regulations, and custom in performing its Fourth Amendment analysis as to the legitimacy of particular expectations of privacy. The Court has adopted such an approach when defining "property" for purposes of its procedural due process analysis. Bell, *supra* note 11, at 774-75.

¹⁹⁷ In the context of civil claims against banks for breach of confidentiality, state courts have found that account holders enjoy an expectation of privacy that imposes upon banks legally enforceable obligations to keep information confidential. *Suburban Trust Co. v. Waller*, 408 A.2d 758, 764-65 (Md. Ct. Spec. App. 1979); *Peterson v. Idaho First Nat'l Bank*, 367 P.2d 284, 290 (Idaho 1961); *Tournier v. Nat'l Provincial & Union Bank of Eng.*, 1 K.B. 461 (1923).

¹⁹⁸ These particular rulings have been limited legislatively. Bell, *supra* note 11, at 794-95 & nn.222-23.

¹⁹⁹ Indeed, Congress essentially took steps in this direction in enacting the Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, §§ 1100-1122, 92 Stat. 3641, 3697-3710 (codified at 12 U.S.C. §§ 3401-3422 (2000)), governing confidential banking records, and the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.), governing the use of pen registers and similar devices to obtain communications attributes. Of course, in those statutes Congress imposed a far less demanding standard than that suggested above.

confidence.²⁰⁰ However, that cause of action was not successfully transplanted in the United States.²⁰¹ Several writers have suggested a greater emphasis on breach of confidence cause of action and laid out their proposals for a breach of confidence action in American jurisdiction.²⁰²

Such a cause of action would surmount the consent defense typically raised by those who engage in deceit and cabin use of undercover techniques. Moreover, such an approach, focusing on the relationships with people to whom we divulge information, fits our intuitions that some relationships warrant more protection than others (and that privacy is not an interest individuals have either with respect to everyone or no one).²⁰³ The relationship between a cab driver and his fare, between two close personal friends, between a bank and a depositor differ dramatically in terms of privacy expectations. Privacy legislation increasingly focuses on limiting dissemination of records held by entities that have certain relationships with individuals, creating a type of confidentiality between them. For example, federal statutes and regulations limit video rental stores, doctors, and educational institutions from divulging their patrons' records.²⁰⁴ Courts could impose civil liability upon journalists and other public citizens who establish or use certain relationships to obtain a person's confidences.

I have discussed the confidential relationship mode of privacy analysis in terms of protecting information individuals entrust to others. Moreover, the discussion has focused primarily on commercial relationships. However, private non-commercial associations play a critical role in individuals' mental health and enhance their autonomy. The Supreme Court has recognized the critical importance of private associations, even those that, unlike religious institutions, receive no explicit recognition in the Constitution.²⁰⁵ The Court has observed: "[C]ertain

²⁰⁰ Susan M. Gilles, *Promises Betrayed: Breach of Confidence as a Remedy for Invasions of Privacy*, 43 BUFF. L. REV. 1, 9-15 (1995); G. Michael Harvey, Comment, *Confidentiality: A Measured Response to the Failure of Privacy*, 140 U. PA. L. REV. 2385, 2395-97 (1992); Alan B. Vickery, Note, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426, 1453-54 (1982).

²⁰¹ American courts have generally not adopted such a broad cause of action. *But see* *Corliss v. E.W. Walker Co.*, 64 F. 280 (C.C.D. Mass. 1894). Gilles also notes that some breach of confidence actions have been recognized in California and New York, and decisions in other states have suggested possible receptiveness. These actions, however, have largely involved fiduciary relationships or commercial arrangements. Gilles, *supra* note 200, at 53-58. *See generally*, DAVID A. ELDER, *PRIVACY TORTS* §§ 5:-5:3 (2002).

²⁰² Gilles, *supra* note 200, at 76-83; Harvey, *supra* note 200, at 2422-49; Vickery, *supra* note 200, at 1455-68.

²⁰³ *See supra* note 195.

²⁰⁴ *See supra* notes 57-59 and accompanying text.

²⁰⁵ In several cases defining First Amendment freedom of association, the Court has recognized private associations as valuable and acknowledged that they merit some respect from government. *See Bd. of Dirs. of Rotary Int'l v. Rotary Club of Duarte*, 481 U.S. 537,

kinds of personal bonds have played a critical role in the culture and tradition of the Nation by cultivating and transmitting shared ideals and beliefs; they thereby foster diversity and act as critical buffers between the individual and the power of the state."²⁰⁶ Accordingly, such groups should receive some protection from infiltration. Thus private associations warrant protection not merely because a particular member's confidences might otherwise be compromised, but also because affording such protection will allow such associations to develop free from government, or other outside, interference. In the undercover context, for instance, this interest might at least serve to bar third parties from using deceit to infiltrate groups.

Several considerations, however, suggest the need for caution in recognizing relationships as confidential in a way that both precludes others from disingenuously forming such relationships with targets in order to gain information, and prohibits those who sincerely entered such relationships from later deciding to disclose information gained during the relationship.

First, to the extent there is a sincere relationship followed by a falling out between confidant and confider, a robust confidentiality doctrine could severely constrain the confidant's own freedom of self-expression regarding significant aspects of her own life.²⁰⁷ Recall *Haynes v. Alfred A. Knopf, Inc.*,²⁰⁸ a case discussed earlier. As noted earlier, journalist Nicolas Lemann's *The Promised*

545-46 (1987); *Roberts v. United States Jaycees*, 468 U.S. 609, 619 (1984); *NAACP v. Alabama*, 357 U.S. 449, 460-61 (1958). Courts have recognized associational rights even when doing so frustrates attainment of goals of the highest order, such as ending racial and gender discrimination. Indeed, some have raised the threat that undercover operations pose to freedom of association as a basis for declaring undercover techniques violative of the Fourth Amendment. See *United States v. White*, 401 U.S. 745, 762-65 (1971) (Douglas, J., dissenting); *id.* at 787-89 (Harlan, J., dissenting); *United States v. Jannotti*, 673 F.2d 578, 612-13 (3d Cir. 1982) (Aldisert, J., dissenting); *FBI Undercover Guidelines: Oversight Hearings Before the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary*, 97th Cong. 4, 47 (1981) (testimony of Geoffrey R. Stone and Gary T. Marx).

²⁰⁶ *Roberts*, 468 U.S. at 618-19; see also MICHAEL J. SANDEL, *DEMOCRACY'S DISCONTENT: AMERICA IN SEARCH OF A PUBLIC PHILOSOPHY* 93 (1996); ALEXIS DE TOCQUEVILLE, *DEMOCRACY IN AMERICA* 513-17 (J.P. Mayer ed., George Lawrence trans., Anchor Books 1969) (1835).

²⁰⁷ Jack Dolan, *Bridgeport Hospital Drops Suit*, THE HARTFORD COURANT, July 27, 2002, at A1 ("How can you prevent somebody from talking about what happened to their dead spouse? An agreement like that would never be valid."); Jim Dwyer & Ford Fessenden, *Lost Voices of Firefighters, Some on the 78th Floor*, N.Y. TIMES, Aug. 4, 2002, at A1:

The department has identified the voices of at least 16 firefighters [who died on September 11, 2001 in the collapse of the World Trade Center] on the tape, and . . . their families were invited to listen to it [but were first] required to sign a statement . . . saying they would not disclose the last words of their husbands, brothers and sons.

²⁰⁸ 8 F.3d 1222 (7th Cir. 1993).

Land, a book about the Great Black Migration used the relationship between two ordinary people caught up in that movement, Ruby Lee Daniels and Luther Haynes, to illustrate the author's themes. Haynes, who had, by the time of the books' publication, turned his life around, was described as a hard-drinking, abusive ne'er-do-well. This account came from Daniels, whose description of her experiences included very intimate details of the couple's marriage.²⁰⁹ Had Haynes been able to sue Daniels for breach of confidence, rather than bring the suit he brought for disclosure of private facts against the book's publisher, Daniels would have been precluded from describing defining moments of her own life essential to the development of her own personality.²¹⁰

Such concerns are hardly fanciful. Some celebrities require their spouses to sign confidentiality agreements.²¹¹ Such agreements can potentially prohibit the spouse from recounting not only purely titillating matters, but also wrongs done to them in the course of the relationship.

Perhaps this objection could be overcome by crafting a defense to any breach of confidence cause of action. In other contexts, confidentiality obligations do not prohibit the confidant from revealing a confidence to protect his own "superior" interest. Thus an attorney may reveal a confidence in defending a malpractice action.²¹² Perhaps that principle could provide the basis for an exception to confidentiality obligations that allows confidants to breach confidences, when necessary, to either comment on wrongs done to them or recount defining elements of their life story.

Second, to the extent a real relationship existed at some point, confidentiality obligations place unfair strains on the confidant, who may have conflicting duties or who may merely not wish to become complicit in wrongdoing. For instance, recently a Catholic priest bound by the seal of the confessional revealed that for a period of several years he could not provide authorities with information that would have freed an innocent person from incarceration.²¹³ A more prominent figure,

²⁰⁹ *Id.* at 1224–25.

²¹⁰ Anita L. Allen, *Lying to Protect Privacy*, 44 VILL. L. REV. 161, 164 (1999) ("Feminists have warned that to advocate privacy aggressively is to advocate that men be allowed the freedom to subordinate women behind closed doors."); see also CATHERINE A. MACKINNON, *FEMINISM UNMODIFIED: DISCOURSES ON LIFE AND LAW* 96–102 (1987) ("When the law of privacy restricts intrusions into intimacy, it bars change in control over that intimacy."); TURKINGTON & ALLEN, *supra* note 108, at 15.

²¹¹ Alan E. Garfield, *Promises of Silence: Contract Law and Freedom of Speech*, 83 CORNELL L. REV. 261, 265–66 (1998).

²¹² MODEL RULES OF PROF'L CONDUCT R. 1.6(b)(3) (2002); RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 64 (2000); RESTATEMENT (SECOND) OF AGENCY § 395 cmt. f (1958) ("An agent is privileged to reveal information confidentially acquired by him in the course of his agency in the protection of a superior interest of himself or of a third person.").

²¹³ See *Morales v. Portuondo*, 154 F. Supp. 2d 706, 710 (S.D.N.Y. 2001) (stating that a priest and lawyer could not reveal the confession of a person to a crime for which two other

Jeffrey Wigand, faced a similar dilemma. Wigand concluded that the tobacco company for which he formerly worked had concealed its knowledge of nicotine's harmful effects. However, a confidentiality agreement Wigand had signed, as a condition of employment, when he first joined the company precluded him from disclosing such information, which he believed had significant public importance.²¹⁴ Surely society should not widely impose upon citizens such traumatic dilemmas.

Third, widely applicable confidentiality obligations would harm the public interest. In particular, they would endanger the autonomy of others who should be able to make fully informed decisions about whether and on what terms to interact with others.²¹⁵ The controversy regarding sealed settlements or sealed discovery materials in products liability cases illustrates this problem.²¹⁶ Such concerns have recently led the American Bar Association to amend its model rules of ethics to give attorneys greater discretion to breach confidentiality when their client's conduct poses the risk of life-threatening injury to others.²¹⁷

Fourth, a confidentiality obligation (or at least a ban on the use of deception in interacting with others) would prevent individuals from protecting themselves. The people and entities with whom we deal may act duplicitously and treat us unfairly

individuals were being incarcerated).

²¹⁴ In Wigand's case the issue was not Wigand's unwillingness to breach his confidentiality agreement and disclose his former employer's "confidences" — he was all too willing, but rather whether his employer could sue media entities for inducing Wigand's breach of contract. See *Brown & Williamson Tobacco Corp. v. Wigand*, 643 N.Y.S.2d 92 (N.Y. App. Div. 1996).

²¹⁵ See generally Garfield, *supra* note 211, at 294–343.

²¹⁶ See Adam Liptak, *Judges Seek to Ban Secret Settlements in South Carolina*, N.Y. TIMES, Sept. 2, 2002, at A1. See generally Laurie Kratky Dore, *Secrecy by Consent: The Use and Limits of Confidentiality in the Pursuit of Settlement*, 74 NOTRE DAME L. REV. 283 (1999).

²¹⁷ Sarah Boxer, *Lawyers Are Asking, How Secret Is a Secret?*, N.Y. TIMES, Aug. 11, 2001, at B7. Compare MODEL RULES OF PROF'L CONDUCT R. 1.6(b)(1) (2002) ("A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary . . . to prevent reasonably certain death or substantial bodily harm . . ."), with MODEL RULES OF PROF'L CONDUCT R. 1.6(b)(1) (1983) ("A lawyer may reveal such information to the extent the lawyer reasonably believes is necessary . . . to prevent the client from committing a criminal act that the lawyer believes is likely to result in imminent death or substantial bodily harm . . ."). Cf. *Tarasoff v. Regents of Univ. of Cal.*, 551 P.2d 334 (Cal. 1976) (holding that a psychotherapist who has determined that his patient presents a serious danger of violence to another has a duty to use reasonable care to protect the intended victim); *Reisner v. Regents of Univ. of Cal.*, 37 Cal. Rptr. 2d 518 (Cal. Ct. App. 1995) (holding that physicians who learned after surgery that transfused blood was HIV-contaminated owed duty to timely warn patient of danger so as to protect third parties from infection); *Pate v. Threlkel*, 661 So.2d 278 (Fla. 1995) (holding that physician had duty to warn patient that patient's condition was genetically transferable and that patient's children should be tested).

and unlawfully. Government will not protect citizens against unfairness short of illegality and does not have the resources to protect us even against all unlawful conduct. In addition, if the government devoted the resources and employed the intrusive techniques needed to protect citizens from pervasive duplicity, citizens might well find the government's efforts unduly intrusive and oppressive. In other words, the pervasiveness of such a government presence would itself be undesirable. Given the constraints on government and the private duplicity that citizens must confront, citizens must be free to engaged in some deception ensure themselves that they are being treated fairly and according to law.

Fifth, a confidentiality obligation, if very broad or inclusive of a wide variety of relationships, may involve the government in trivialities. An individual's minor betrayals of his or her friends' or co-workers' confidences may become lawsuits that must be resolved in court. Legal claims arising out of such common indignities might potentially burden the courts. Moreover, in resolving such cases, courts may have to permit discovery and public discussion of the relationship between the parties that gave rise to the confidentiality obligations. Thus, civil litigation could lead to even greater privacy breaches than allowing minor betrayals of trust to go unpunished.²¹⁸

In short, the confidential relationship mode of privacy analysis has been underutilized in the United States. Constitutional doctrine has systematically ignored relationships between confiders and confidants, treating privacy expectations as ones individuals have equally vis-a-vis all potential intruders. Civil causes of action for breach of confidentiality have not been widely recognized.

²¹⁸ This problem may explain one note writer's suggestion that breach of confidentiality actions lie only to enforce written confidentiality agreements. Such an approach suffers from two problems. First, it would provide protection only by introducing an unfortunate formality into some informal relationship. In some informal relationships the parties implicitly understand each has a obligation of confidentiality to the other. (Such an understanding may be reflected in societal custom or the mutual behavior of the parties involved.) Under the rule, such confidences are protected only if the parties have executed a written agreement. For instance, should those who share sexual intimacies first have to execute a confidentiality agreement before any obligation of confidentiality arises? A refusal to permit confidentiality obligations from arising by implication is particularly troubling in the undercover context. Such a rule would mean that the legally savvy might extract written promises of confidentiality while the untutored would not, even though both were engaged in the same type of relationship with an undercover operative.

Second, it is unfair to allow a person to impose confidentiality on another without first disclosing the confidence to be revealed. The confidant may expect to receive an innocuous confidence and instead receive a confidence that she feels compelled to disclose to avoid complicity in wrongdoing, satisfy a higher duty to someone else, or tell the story of her own life. Needless to say, from the perspective of the public, conferring such a power on individuals to demand that their confidants not disclose those confidences could prove detrimental, by, for example, precluding the public from obtaining critical information.

Wider recognition of such a cause of action might constrain some potentially offensive uses of deception. There are, however, valid reasons for caution in recognizing relationships as having accompanying legal obligations of confidentiality.

F. Databases as a Hybrid Mode of Privacy

A sixth privacy protection mode warrants recognition. Even though it incorporates other modalities of protecting privacy and is in some sense, then, an amalgam of previously discussed modalities, it is often the modality adopted in privacy legislation. In particular, privacy can be protected by protecting the databases from breach by third parties and precluding database custodians from disclosing stored information without consent.

Database protection is a type of location-based protection. By keeping particular records sacrosanct, the privacy of the subjects of that data are protected. The information is protected only against disclosure as a result of the breach of the database — if discovered by some other means it is not protected. However, unlike the modality of physical location, and more like the modality of the means of communication, the important aspect of the database is not its physical location. Rather, the database really has a virtual location.

The database mode of privacy analysis shares some characteristics of the confidential relationship mode of analysis. Database protection is largely accomplished by controlling the custodian of the database, who generally has a relationship with the subject of the record. Database protection is also related to the subject-matter mode of privacy protection. Legislatures protect databases because of the subject matter they contain. Indeed, the statutory protection may focus on particular subject matter within the database. In particular, the legislation is based on the concept that certain types of information should not be made public without an individual's consent. These types of information include the selection of videotapes they rent,²¹⁹ and the public library books they borrow,²²⁰ as well as information provided in connection with driver's licenses,²²¹ educational records²²², and e-mail account records.²²³ Thus, though database protection can be viewed as

²¹⁹ The Video Privacy Protection Act of 1988, Pub. L. No. 10-618, 102 Stat. 3195 (codified at 18 U.S.C. § 2710).

²²⁰ See *supra* note 128.

²²¹ Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, 108 Stat. 2099 (codified at 18 U.S.C. §§ 2721-2725).

²²² Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 88 Stat. 571 (codified at 20 U.S.C. § 1232g).

²²³ 18 U.S.C. § 2703(c) (2000); *McVeigh v. Cohen*, 983 F. Supp. 215, 219 (D.D.C. 1998) (finding military discharge proceedings for homosexual conduct based on the servicemember's anonymous email account profile to be a violation of the Electronic

location based (albeit the location is merely a virtual one) it is not as imprecise or indiscriminate as the classic location-based approaches that focus on protecting a particular physical locations, like residences. Rather it offers targeted protection for particular types of information.

Database protection is generally not defeated by undercover techniques. (It may be, however, generally susceptible to breach by law enforcement authorities and regulators using subpoenas, particularly grant jury subpoenas.) Database custodians would probably not easily succumb to undercover tactics, and those who establish certain relationships using undercover tactics would presumably still be constrained by the relevant statutory obligations. However, because the same information can be obtained from the person to whom the records relate by, among other things, using undercover techniques, database protection does not protect citizens against undercover operations. However, requiring potential intruders to engage in undercover operations against the subject of the information, rather than merely obtaining the information from the records custodian itself, may enhance privacy. Many of the concerns about records organizations maintain on individuals relate to the secondary use of that information and the combination of that information with other information.

CONCLUSION

White-collar crime often involves deception. Sometimes a potent means to uncover the deception, either to punish wrongdoers or to allow others to obtain the information they need to exercise autonomy, is more deception. As noted above, not only do law enforcement officers employ deceptive undercover techniques, but so do a variety of other actors, including administrative agencies, news organizations, and private citizens. We have yet, however, to fully address the privacy implications of the use of deception involved in undercover operations. Indeed, we have more generally had limited success at precisely defining the appropriate sphere or privacy.

As I have suggested in this paper, our analysis of privacy focuses on particular modes of privacy, each of which captures some aspect of privacy by misses others. The dominant modes of judicial protection of privacy, the physical location and subject matter modalities have proven somewhat problematic in general. They have been even more ineffectual in addressing the substantial privacy implications of undercover investigation. Other modes of privacy, focusing on interpersonal relationships, the means of communication, and the means of privacy intrusion, warrant consideration with regard to addressing the implications of undercover operations, and more generally, the dilemmas we face in seeking to secure an appropriate realm of privacy.