balance typically favors withholding records when they are contained in computer compilations, courts don't need to engage in case-by-case balancing with the public interest in disclosure. The simple determination that a record is in a computer compilation was sufficient to withhold it, the court reasoned.

In 2004, the Supreme Court ruled in *Favish v. Office of Independent Counsel*, a case that directly raised privacy and FOIA issues, including the question of the privacy interests of family members of a deceased person. It grew out of requests for photographs taken during the investigation into the death of Vince Foster, a former deputy counsel in the Clinton White House. In 1993, he was found dead in a park in Washington, D.C. The National Park Service, the FBI, committees of the House and Senate, and the Office of Independent Counsel independently investigated. All concluded that his death was a suicide, but rumors and doubts lingered. The District of Columbia Court of Appeals, in 1999, denied the records request of Accuracy in Media, a media watchdog organization, which had requested the photographs from the National Park Service. Allan Favish, a lawyer who had participated in that litigation, renewed the request in California by serving it upon the Office of Independent Counsel, seeking 150 photographs.

The office released more than 100 photos but withheld several for reasons at first not clearly articulated. Favish later dropped twenty-one photos from his request. Eventually the office relied upon the privacy language of Exemption 7. The district court ruled for Favish on one photo and certain issues regarding the quality of the photos but withheld ten to protect the privacy interests of Foster's family. The Ninth Circuit Court of Appeals reversed the district court's ruling and held that, though the privacy interests of the family were a valid consideration, they had to be weighed against the public interest in the investigation. Because the court of appeals did not have the photos in question, the case was remanded to the district court for further analysis and the required balancing of the privacy and access interests. On remand, the district court ordered the release of five photos and withheld, on privacy grounds, the other five. The Ninth Circuit affirmed. In 2004, the Supreme Court reversed the appellate court and held that under the FOIA surviving family members have a right to personal privacy regarding the photographic images of the scene of a close relative's death. The Court said such privacy interests outweighed, under the FOIA, the public's interest in disclosure.

In 2011, in *FCC v. AT&T*, the Court in an 8-0 decision emphatically held that corporations, while protected under the Fourth Amendment from unreasonable searches and seizures, are not shielded under the personal privacy language of Exemption 7 (c) from FOIA requests for documents they provided to government because corporations do not have personal privacy rights and the exemption protects only the privacy of individuals, not businesses.

The Privacy Act of 1974

The Privacy Act was meant to create a "Code of Fair Information Practices" to regulate government agencies. The Senate report on the legislation noted that one purpose of the act was "to promote government respect for the privacy of citizens" by ensuring that executive branch agencies follow certain rules regarding the gathering and disclosing of information. The Privacy Act is most likely to affect requests for information that is not clearly covered by the legislation. In such cases, custodians of records tend to be very cautious because the Privacy Act imposes penalties on custodians who release protected information. Withholding information that should be disclosed, on the other hand, may violate the federal Freedom of Information Act, but that legislation poses no penalties for wrongly withholding information.

Other Privacy Concerns

A number of other federal and state statutes raising privacy concerns can erect barriers to information gathered and kept by government and, in some cases, private institutions. A few key examples are discussed below.

Driver's Privacy Protection Act. Driver's license records have long been a source of useful information for journalists, more so in recent years with the growth of computer-assisted reporting. In 1991, for example, the *Miami Herald* used a computer analysis of state Division of Motor Vehicle records to show that many drunken drivers were being put back on the road. In 1997, however, federal legislation began limiting access to such records. The law, passed in 1994, was partly in response to the slaying of California actress Rebecca Schaeffer by a fan who located her address through driver records obtained through a private investigator. The intent of the law is to inhibit stalkers and anyone else who might harm an individual after linking a name with an address. The federal legislation contains a provision that allows states to disclose such information if they enact a provision notifying drivers that they have an option to withhold personal information.

Several states challenged the law, arguing that Congress had overstepped its authority in attempting to regulate a state practice. The Seventh and Tenth Circuits of the U.S. Court of Appeals upheld the law. The Fourth Circuit, however, sided with South Carolina, which argued the law was unconstitutional because state driver's license information constituted internal state activity and lay beyond the scope of congressional jurisdiction. The Supreme Court, in *Condon v. Reno*, reversed in 2000 the Fourth Circuit. The unanimous opinion by Chief Justice Rehnquist held that the release or sale of drivers' license information constituted interstate commerce, thereby giving Congress regulatory authority.

The Buckley Amendment. Enacted as the Family Educational Rights and Privacy Act, or FERPA, the Buckley Amendment requires educational institutions receiving federal money to keep certain student records private. Directory information such as names, addresses and majors is not covered. Academic records, including non-criminal disciplinary records, are. Before 1992, the Department of Education advised institutions that campus crime records should be considered student disciplinary records — a position that frustrated many media organizations, particularly campus newspapers. A 1992 amendment, however, states that crime reports are not educational records and cannot be withheld as disciplinary records.

Rape Shield Laws. Whether to publish the name of a rape victim is a controversial topic, both legally and ethically. Rape shield laws were designed to encourage victims to come forward by preventing the additional trauma of publicity. Some courts have upheld such laws. In Florida, however, the state supreme court, in 1994, upheld a ruling that the state's law was unconstitutional in a case spawned by the William Kennedy Smith rape trial. The court relied heavily on *Florida Star v. B.J.F.*, which held the news media should not be punished for publishing truthful, lawfully obtained information about matters of public concern absent a state interest of the highest order.

Juror Shield Laws. Much has been said and written about protecting jurors' privacy, particularly since the Rodney King police brutality and the O.J. Simpson murder trials. Since the Supreme Court's 1984 ruling in *Press-Enterprise v. Superior Court*, jurors' selection and identity have been presumptively public matters. But after the King and Simpson cases, and the Timothy McVeigh trial in the Oklahoma City bombing, the tide began to change. Citing privacy, judges appear to be routinely impaneling anonymous juries, a practice once reserved for the trials of organized crime kingpins when juror safety was a factor; and some states have passed laws expressly allowing the practice.

Computer Privacy. Journalists depend increasingly on information contained in computer databases, the World Wide Web and other computer-based sources. Indeed, going online is allowing journalists greater speed and access to more information. Many significant news stories are based on an analysis of government databases. Most laws dealing with computer privacy are designed to place limits on government. The Computer Matching and Privacy Act of 1988, for example, limits the ability of government to routinely cross-reference information in various government databases. The Electronic Communications Privacy Act of 1986 made the interception of computer communications a crime, and the Computer Crime Act of 1986 made it unlawful to access or disclose certain records in computer form. Many of the laws, reflecting some of the constitutional and statutory concerns discussed previously, treat computerized information as more threatening to privacy than similar information in paper files. Such laws can be vague or over-inclusive in ways that inhibit legitimate journalists.

The computer/privacy debate also has begun to focus on private-sector information practices. In 2000, after conducting a series of Web site surveys, the FTC abandoned its long-standing policy supporting self-regulation. Instead, it announced support for federal legislation to protect online consumers, much to the dismay of the Online Privacy Alliance, an informal industry coalition that included some of the biggest online companies. FTC officials recommended that Congress establish standards regarding online information collection. More recent controversies have focused on the search information, email and personal identifiers retained by companies such as Google (including YouTube) and various cellular telephone providers.

In 2014, the Pew Research Center published a study that indicated most people are generally not worried about the collection of their search information and receipt of targeted advertising if that's the price for getting certain online services at no cost, though many also indicated some concerns about tracking geographic locations through mobile devices.

A growing privacy concern involves the posting of diary entries and other information by individuals on online social networking sites such as Facebook and LinkedIn. Many students and others have found that once information is posted and widely shared, the expectation of privacy lessens. Employers, government agencies and others have used these sites to gather information about individuals. In 2007, Facebook triggered substantial public criticism with its Beacon advertising program that transmitted users' online purchasing information to their friends on the social network. Facebook ultimately changed the program, added an opt-out feature, and apologized to its users. Of course, these issues with Facebook, Twitter and other social media sites as well as search engines continue to arise here and elsewhere in the world as the technology changes.

Social media sites, search engines, business interests and individual consumers have increasingly engaged in online conduct that may erode or at least alter societal expectations and norms regarding personal privacy. Facebook's various privacy policies and controversies, Google's retention of search histories and user information, cell phone tracking capabilities, and even cable companies and other companies that can read, block or track certain types of messages all stand to change traditional notions about what is private and what is not.

In 2012, Facebook entered into a $9.5 million settlement with a class of its members who had sued over the site's Beacon program (started in 2007) that effectively gathered and disseminated information about Facebook members' online activities without their consent. In addition to the payment, which went to attorney's fees and to set up a new foundation dedicated to user education and protection of online identities, Facebook agreed to end the Beacon program.

The conflict over what privacy rules or laws apply to the online collection of personal information by commercial sites is likely to continue as new government agencies enter this arena and as more people look for ways to control their own data.

In a reminder that the world is shrinking, Google in 2014 hit the so-called "right to be forgotten" wall in Europe when the European Court of Justice ruled that it must comply with local law on such a right and thus will have to remove, after a process, certain items from its search results. The results are potentially dramatic not only for the giant search engine's business model, but for fundamental notions of public access to information as well, showing once again that on privacy matters Europe and the United States are two related, but very different legal worlds.

Health Insurance Privacy. The privacy rules under the Health Insurance Portability and Accountability Act of 1996 took effect in 2003. They do not directly apply to the media, but they do affect many businesses, including hospitals. They probably are more likely to refuse to release information about patients or even to confirm that an accident victim has been admitted. In addition, the law may influence the tone and direction of future privacy legislation.

The HIPAA rules limit the use and disclosure of individuals' health information by doctors, hospitals, health-care clearinghouses, insurance plans, their business associates, and many employers who provide health care or coverage. For example, employers may not use the information to make personnel decisions, and any covered entity may only disclose the information for purposes related to treatment, payment and health care operations, unless the individual has provided a clear, voluntary authorization permitting disclosure. The rules also require that each covered business adopt privacy procedures and train a designated privacy official to assure compliance.

The rules do not provide for private lawsuits seeking enforcement but do provide for investigations by the Department of Health and Human Services, which can then seek civil and criminal penalties for violations. Examples of exceptions allowing disclosure, even without authorization by individuals, include public health investigations, law enforcement, emergencies and national security; but there is no exception for any reports to journalists — even for the release of limited information concerning admission and discharge dates of patients.

The law and its consequences took on new importance with the 2014 reporting on the Ebola story, causing journalists to attempt to balance patient privacy with needed reports to the public. Hospitals were typically advised that they could release general information without patient names in an effort to keep people informed about possible risks of exposure.

A recurring problem with HIPAA has been the level of misunderstanding of the law by health care providers that fear claims over disclosures and therefore err on the side withholding too much information — even from close family members of patients. If family members experience these problems, journalists are certain to fare even worse.

Privacy After September 11, 2001

The terrorist attacks that took place on September 11, 2001, have had a far-reaching impact on society, laws and notions of privacy. These matters are still evolving. Interestingly, some government officials responsible for security matters have recently argued that privacy can no longer be equated with anonymity in terms of personal information and private communications. They contend that government must have greater access, particularly to certain telecommunications and financial information, to guard against terrorist and criminal acts and that the focus of privacy advocates should be on the creation of legal safeguards limiting the permissible uses of that information by government.

The USA PATRIOT Act increased federal authority in a number of ways. It relaxed restrictions on the sharing of information between domestic law enforcement agencies and intelligence agencies, enhanced the government's subpoena power to obtain and inspect email records of suspected terrorists, expanded bank record-keeping requirements to track transactions and money laundering, and permitted roving wiretaps of suspected terrorists. More than 300 pages long, the law received virtually no debate or congressional oversight before its passage. The sense of urgency and fear following the attacks and the fact that the law included a provision for its sunset in five years facilitated its quick enactment.

Not long after his reelection in 2004, President George W. Bush began urging renewal of expiring PATRIOT Act provisions as well as expansion of certain powers of government to obtain records without judicial approval. After months of negotiations with Congress and amid media reports of secret government wiretapping of international telephone calls, a compromise was reached in 2006. The act was renewed with a few modifications limiting some government powers to obtain routine library records and providing people served with terrorism-related subpoenas the right to challenge the nondisclosure and gag order requirements of the subpoenas. The renewal, though, made permanent most of the PATRIOT Act's provisions.

In 2008, President Bush and Congress squared off and then compromised regarding a major expansion of government's power to conduct surveillance, including a significant revision of the thirty-year-old Foreign Intelligence Surveillance Act and its rules governing the liability of telecommunications companies that facilitated secret and possibly illegal government wiretaps after the 2001 terrorist attacks. As part of the compromise, Congress included in the new law immunity for the telecommunications companies that had cooperated with the government in conducting warrantless wiretaps, a hotly contested issue that

nation — even from close family mem-
ly members experience these problems,
fare even worse.

11, 2001

took place on September 11, 2001,
pact on society, laws and notions of
still evolving. Interestingly, some
ible for security matters have re-
n no longer be equated with ano-
nformation and private communi-
overnment must have greater ac-
elecommunications and financial
terrorist and criminal acts and
ates should be on the creation of
permissible uses of that infor-

reased federal authority in a
ictions on the sharing of infor-
orcement agencies and intelli-
ernment's subpoena power to
of suspected terrorists, ex-
ements to track transactions
tted roving wiretaps of sus-
ages long, the law received
al oversight before its pas-
following the attacks and
vision for its sunset in five

004, President George W.
PATRIOT Act provisions
of government to obtain
r months of negotiations
ts of secret government
calls, a compromise was
with a few modifications
ain routine library rec-
terrorism-related sub-
closure and gag order
val, though, made per-
ions.
squared off and then
of government's pow-
ficant revision of the
illance Act and its
nications companies
overnment wiretaps
f the compromise,

led to prompt but unsuccessful legal challenges. In 2011, Presi-
dent Obama signed a four-year extension of the PATRIOT Act
as previously amended. But in 2015 the law and the practice of
collecting in bulk data about the telecommunications of Ameri-
cans hit a legislative and judicial snag as key provisions of the
act were challenged and then expired for lack of a legislative
deal on revisions and an extension.

During the coming years, the pressure to invest government
with new powers and to use computer technology and the Inter-
net to track and prevent terrorism will continue to be strong.
The results may include not only a contraction of the privacy
rights of individuals, but also a contraction of sources of infor-
mation available to journalists. The controversies that arose in
2013 and 2014 as a result of Edward Snowden's disclosures of
data-mining by the National Security Agency only made more
obvious the potential impact of new technology on what once
seemed to be settled notions of privacy. While many continue to
debate the exact nature of the NSA's data collection and the
impact of the Snowden revelations on national security, there is
no doubt that the furor over the NSA will fuel privacy debates,
new guidelines and a fresh look at government surveillance. In
2018, for example, the NSA announced it had purged hundreds
of millions of records logging phone calls and texts that it had
gathered from domestic telecommunications companies since
2015, apparently because the collection include files it was not
allowed to receive.

SUMMARY

Despite assaults on their privacy from various quarters — and perhaps in part because of those assaults — Americans remain strong in their belief in the right to be let alone. Privacy concerns are manifested in constitutions, statutes and common law cases that attempt to balance individual rights with competing values, including the right of the news media to publish and the right of the public to be informed. It is to be expected that the rights of individuals and of a free and vigorous press often will clash. The balance has generally tilted toward the press because of the bedrock principle that a democratic society works best when information flows freely.

Journalistic excesses are not lost on the public, whose declin-
ing opinion of journalism has been reflected in some polls. The
results of declining confidence can be seen in the outcome of
some court cases. Lack of public confidence in the news media
also can embolden politicians to pass laws limiting press free-
doms in the name of privacy.

BIBLIOGRAPHY

Articles

Law Review 29 (2011).
Coleman, A.D. "Private Liv
raphy Ethics," 2 *Journal*
/Summer 1997).
Editorial, "The Telephone Ur
1877, at 4.
Hopkins, W. Wat. "Snyder v.
of Intentional Infliction of
Based Tort," 3 *Journal of*
https://law.ubalt.edu/acad
Prosser, William. "Intention
New Tort," 27 *Michigan L*
Prosser, William. "Privacy,
(1960).
Smith, Jeffery A. "Moral Gu
to Privacy," 10 *Journalism*
63 (2008).
Warren, Samuel D. & Louis
cy," 4 *Harvard Law Revie*
Woo, Jisuk. "The Right Not
nymity in the Interactive
Society 949 (2006).

Books

Ernst, Morris, & Alan Schv
Alone, London: MacGibbo
Flaherty, David H. *Privac*
lottesville: University Pre
Glasser, Charles, ed. *Intern*
New York: Bloomberg Pre
Hixson, Richard F. *Privacy*
in Conflict. New York: Ox
Locke, John. *The Second*
Peardon, ed. Englewood
Mill, John Stuart. *On Liber*
York: Macmillan, 1956.
Pember, Don. *Privacy an*
Washington Press, 1972.
Restatement (Second) Torts
Rule, James B. *Privacy in*
damental Right in Exch
New York: Oxford Unive
Westin, Alan F. *Privacy a*
1967.

Cases

Anderson v. Gannett Co., 9
Gannett Co. v. Anderson
Armstrong v. H&C Commu
(Fla. Ct. App. 19