RESEARCH ETHICS

J. Heal Ethics Admin
Volume 12 | Number 3 (Summer 2026)
www.jheaonline.org
ISSN 2474-2309 | doi:10.22461/jhea.1.71657
https://doi.org/10.22461/jhea.1.71657
Published Aug 10, 2026

REGULATING RESEARCH USE OF INFORMATION: PUBLIC, PRIVATE, OR SOMETHING ELSE?

Ivor A. Pritchard, Ph.D.

ivor.a.pritchard@gmail.com

Abstract: *This essay analyses how the concept of 'privacy' is construed in determining the U.S. regulatory approach to research involving human subjects. It begins by setting out how the federal policy for the protection of human research subjects - also known as the Common Rule - identifies privacy, showing how the Common Rule's rendering of the concept is fundamentally incomplete. It then describes how modern technology has expanded the wealth of information that might be considered private, at the same time as it has moved further into the realm of what has been considered private, offering investigators new opportunities to look into various aspects of people's lives. The essay then uses some key U.S. Supreme Court decisions turning on the idea of a right to privacy alleged to be embedded in the Constitution of the United States to illustrate how the concept has evolved in response to technological developments in the generation and transmission of information. Based on these considerations, I proceed to argue that classifying all information as either 'public' or 'private' is inadequate, and that the regulated research community and the public at large should directly address the challenges of how to use information that is neither public nor private, but rather 'restricted social information (RSI)'. This in turn implies that there is human behavior that is neither public nor private, which should be classified as 'restricted access social behavior' (RASB). And this affects the question of what is left of privacy, and how investigators should approach the investigation of what is truly private. I offer recommendations for regulatory revisions to the Common Rule, considering the views of some of the leading theorists about privacy.*

Keywords: *Privacy, Digital Privacy, Regulatory Privacy, Privacy and Secondary Research, Common Rule.*

*Address correspondence to: Ivor A. Pritchard, Ph.D. Email: ivor.a.pritchard@gmail.com

+To cite this article: Pritchard, I. "Regulating Research Use of Information: Public, Private, or Something Else?". The Journal of Healthcare Ethics & Administration Vol. 12, no. 3 (Summer 2026): 18 -37, https://doi.org/10.22461/jhea.1.71657

INTRODUCTION

Research using personal information is a burgeoning industry. While randomized clinical trials may be considered the gold standard for establishing research findings, research uses of personal information based on secondary analyses of data enable investigators to investigate a wealth of questions far beyond what clinical trialists could even dream of, and research combining information measuring interventions' effects with other information is also widespread. The technological development of the computer, internet, and electronic databases and repositories over the past several decades have revolutionized the ability to access and analyze information of all sorts in the biomedical, behavioral, and social scientific realms, and beyond. Much - but not all - of that personal information is considered to be 'private', posing regulatory and confidentiality concerns and raising questions about whether anything is truly private anymore.

This essay analyses how the concept of 'privacy' is construed in determining the U.S. regulatory approach to research involving human subjects. It begins by setting out how the federal policy for the protection of human research subjects - also known as the Common Rule - identifies privacy, showing how the Common Rule's rendering of the concept is fundamentally incomplete. It then describes how modern technology has expanded the wealth of information that might be considered private, at the same time as it has moved further into the realm of what has been considered private, offering investigators new opportunities to look into various aspects of people's lives. The essay then uses some key U.S. Supreme Court decisions turning on the idea of a right to privacy alleged to be embedded in the Constitution of the United States to illustrate how the concept has evolved in response to technological developments in the generation and transmission of information. Based on these considerations, I proceed to argue that classifying all information as either 'public' or 'private' is inadequate, and that the regulated research community and the public at large should directly address the challenges of how to use information that is neither public nor private, but rather 'restricted social information (RSI)'. This in turn implies that there is human behavior that is neither public nor private, which should be classified as 'restricted access social behavior' (RASB). And this affects the question of what is left of privacy, and how investigators should approach the investigation of what is truly private. I offer recommendations for regulatory revisions to the Common Rule, considering the views of some of the leading theorists about privacy.

THE REGULATORY SIGNIFICANCE OF PRIVATE IN THE COMMON RULE

'Private' is a key term used for determining the applicability of the U.S. Federal Policy for the Protection of Human Subjects (aka the Common Rule) to research studies (HHS 2017). Whether or not there is any interaction or intervention with subjects, obtaining and using "identifiable private information" in a federally supported research study brings the research under the requirements of the policy, unless the research study fits within an exemption.
The 2018 revisions to the Common Rule draw additional specific attention to the concept of privacy in two important ways. First, the federal government is charged with periodically re-examining the meaning of "identifiable private information", determining whether emerging analytic techniques or technologies should be considered to generate identifiable private information or identifiable biospecimens, and publishing a list of these technologies and techniques for public awareness (HHS 2017, 45 C.F.R. § 46.102(e)(7)(i-ii)). Presumably this re-examination will alter the scope of what is considered "identifiable private information", influencing whether a study falls under the Common Rule. And second, the Secretary of the Department of Health and Human Services, (HHS) in consultation with other federal offices, is charged with issuing guidance on the protection of privacy and maintaining confidentiality of data, which should provide additional explanation of what privacy is (HHS 2017, 45 C.F.R. § 46.111(a)(7)(i)). But neither of these tasks has actually been accomplished, or even publicly initiated, so far.

While considerable attention has been devoted to scrutinizing what counts as *identifiable* and *re-identifiable* data, the regulatory research community appears to have paid less attention to identifying what should be considered *private,* despite the fact that there has been active scholarship over the last few decades regarding the

meaning of privacy (Mason 2024; Wisniewski & Page 2022). The meaning of privacy is far from obvious or transparent; it has varied and been used in different ways over time and across cultures, and the evolution of information technology has significantly affected the boundaries of what people view as private, leading some to assert that privacy no longer exists.

The Common Rule approaches the concept of privacy through its definition of "human subject", as follows:

> (e)(1) Human subject means a living individual about whom an investigator (whether professional or student) conducting research:
>
> > (i) Obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or
> > (ii) Obtains, uses, studies, analyzes, or generates identifiable *private* information or identifiable biospecimens [italics added] (HHS 2017, 45 C.F.R. § 46.102(e)(1))

It then goes on to describe "private information" as follows:

> (4) Private information includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information that has been provided for specific purposes by an individual and that the individual can reasonably expect will not be made public (e.g., a medical record) (HHS 2017, 45 C.F.R. § 46.102(e)(5)).

This is not a definition of 'private', or if it is, it is seriously flawed: it provides two criteria for kinds of information that are "included" in what is private, but does not provide criteria or boundaries regarding what other information is private. This is like defining 'animal' by saying that the term 'includes birds and fish' but not identifying any comprehensive criteria or standard, or identifying what other kinds of critters are satisfactory candidates. And there are indeed other likely candidates of privacy: For example, many of the thoughts and feelings that we never express or exhibit through behavior are presumably private, and information about them should also be included as patently private, but they do not satisfy either of the criteria.

The two criteria given are also problematic. Regarding the first criterion, not all behavior that occurs in a context where there is no observation or recording taking place is private: For example, a nighttime janitor's work activity in a building with no monitoring devices is difficult to think of as private behavior. Un- recorded jury deliberations and other closed-door meetings and activities of various kinds where recording does not occur are also not 'private' in the strict sense. Regarding the second criterion, individuals may disclose information to others and swear them to secrecy, even if they do so with no specific purpose in mind, and this would likely be considered private. On the other hand, if an individual casually discloses information about themselves in the course of a social transaction of some kind and does not expect that the person to whom they disclosed the information would re-disclose it, but they do, it is difficult to see that such events are always violations of the first individual's privacy. In sum, the regulatory descriptors do not satisfactorily separate off what is private from what is not.

The Common Rule provides a few other signals about the meaning of private. In two of the exemptions from the requirements of the Common Rule, it refers to "…observation of public behavior" and to whether "…The identifiable private information or identifiable biospecimens are publicly available." (HHS 2017, 45 C.F.R. § 46.104(d)(2) & (4)(i)) Here it is evidently distinguishing the private and the public, although it is arguable that some information could be both publicly available and private, as when a hacker posts hacked guarded identifiable personal information online on a public website.

The Common Rule refers to public and private information, and seems to assume that information that is not public is automatically private. But what if that is not so? What if there is information that is not freely available through unrestricted access, on request, or for a nominal fee, but is also not private in some meaningful sense? What if there is information the access to which is controlled, limited, and guarded in some way, but still should not be considered 'private'? Likewise, what if there is also human behavior the access to which is controlled, limited, and

guarded in some way, but still should not be considered 'private'? This essay will assert that such information and behavior are abundant, and that research uses of such information should follow regulatory standards that are neither the same as those for publicly available information nor those for truly private information. We will call this information 'restricted social information'(RSI). And I shall also claim that there are various arenas for behavior that is neither public nor private, the status of which should be addressed explicitly by the Common Rule and which we will call 'restricted access social behavior'(RASB). But first, some attention should be paid to sketching out the landscape of existing personal information, which has expanded considerably, making the existence of RSI far more obvious.

PRIVACY, TECHNOLOGY, AND RESEARCH ACCESS

Researchers are frequently interested in gaining access to information that was originally generated for some nonresearch purpose, in order to pursue a scientific question. Researchers' main objective in accessing individuals' information ordinarily transcends those individuals' personal interests, to focus on the answers to scientific questions about populations in general. If the research involves interventions with subjects, those interventions may benefit, harm, alter, or have no lasting effect on the subjects. If the research only involves information about the subjects, the researchers may share results with subjects, either because it might be useful to them, or as a gesture of respect or gratitude for their participation. The researcher's primary objective is to use the information to answer a scientific question, while limiting the access and use of that information to the scientific analysis so that subjects go unexposed and unharmed. Their interest in the subjects' welfare is contingent, external to their scientific purposes. So long as protecting research subjects and the information they gain about them does not pose too great a burden, researchers have an interest in not harming or offending research subjects so that researchers can continue to pursue their objectives of obtaining and analyzing personal information without creating additional obstacles or objections.

Technology is dramatically transforming the opportunities for researchers to perform research using electronically generated, transmitted and stored information. The telephone landline became an alternative to private letters, and cell phones, texting and email functions have in turn become alternatives to the landline. Cell phones track the online behavior of their users and a considerable portion of their behaviors and movements in the physical world. Widely employed cameras and portable devices also monitor and record people's movements, sometimes without their notice or awareness. Social media have proliferated exponentially, enabling anyone with access to a cell phone or computer to post information about themselves or others to the wide open public or to select groups. Computers and the internet have made it possible to effortlessly digitize, store and transmit personnel records, financial records, health records, education records, dating records, recreational records, government records, criminal records, etc.. Online shopping tracks what people look at, and what they acquire.

As a condition of individuals' access to a vast array of online platforms, users are routinely required to accept an end-user licensing agreement (EULA), and/or a terms of privacy agreement, which identifies at great length and in virtually unintelligible language the conditions under which the platform may use and share the users' information. The overwhelming majority of users are unaware of the specifics of these agreements, or have even tried to read them. U.S. Supreme Court Justice Alito has pointed toward the public's vulnerability in this regard:

> The Fourth Amendment restricts the conduct of the Federal Government and the States; it does not apply to private actors. But today, some of the greatest threats to individual privacy may come from powerful private companies that collect and sometimes misuse vast quantities of data about the lives of ordinary Americans (Carpenter v. U.S. 2018, 17-18).

It is also important to note the ways in which individuals themselves are affected by the transformational innovations of technology. As the philosopher Hannah Arendt noted in a different context, technological change can dramatically amplify and reshape the consequences of what humans do; Arendt originally made this point with regard to how invented weapons increase the human capacity to perform violence (Arendt 1970). And at the same time, she pointed out that the use of these technologies takes away from the agent the ability to directly perceive

those magnified effects with the unaided senses. The same may be said for information technology: the awareness of writing and posting a personal letter to someone is dramatically different from the awareness of sending an email or text. Where the content of that email or text will end up is also potentially far greater. This can also be said for sending a printed photograph through the mail versus posting a picture on a social media platform.

Take email, for example. In his dissent in the case of *Carpenter v. the United States,* U.S. Supreme Court Justice Gorsuch commented that "Whatever may be left of *Smith* and *Mille*r, few doubt that e-mail should be treated much like the traditional mail it has largely supplanted – as a bailment in which the owner retains a vital and protected legal interest" (Carpenter v. U.S. 2018, p.15) While Gorsuch may be correct with respect to the legal status of e-mails, in practical reality the vulnerability of e-mails to broad exposure is drastically otherwise. The e-mails are stored on a server to which administrators have access, and recipients' ability to forward an e-mail, again and again, to who knows who, occurs at the click of a mouse. Many working employees use office individual e-mail accounts to send personal messages while on the job, and their ability to send those e-mails is conditioned by the terms of their employer; for example, U.S. federal employees logging onto their government computers are informed that "THERE IS NO RIGHT TO PRIVACY IN THIS SYSTEM". Those employees may or may not pay attention to that warning, but in any event any member of the outside public who sends an email to a federal employee is not cautioned in the same way to be careful about the content of what they send into that system.

Researchers are investigating human behavior online which may differ significantly from human behavior in face-to-face interactions. For example, the *online disinhibition effect* is a term coined for the various ways in which people express themselves more freely online (Suler 2004). Interacting via a computer is also alleged to encourage various forms of regressive behavior (Holland 1996). Researchers have found that controversial information travels faster and further through certain online social networks than noncontroversial information (Jassar, Gariby, et.al. 2022, 111-122). People sharing information about themselves are often unaware of what they share, who they share it with, and how it can be used, and are readily influenced by the ways in which their sharing choices are framed (Acquisti et.al. 2015, 509-514). In an ethically infamous research study, researchers demonstrated that controlling the flow of information on social networks (Facebook, specifically) could be used to affect users' emotional behavior (Kramer et al. 2014, 8788-8790). In a recent report, the Surgeon General raised concerns about the ways in which online experiences may influence the lives of vulnerable adolescents (Murthy 2023). Clearly, research using information online holds considerable potential for understanding the distinctive qualities of human behavior in the spaces created by information technology, some of which the users might think of as private.

In sum, the technological evolution and use of information has created a vast landscape of information about people where researchers may pursue all sorts of interesting research questions about individuals and their behavior, often without those individuals' awareness of the researchers' scrutiny. Individuals are far less aware of the ways in which information about them goes out into the world, and users - including researchers - have far easier access to the vastly increased amount and kinds of information about them. The information may expose them in more sensitive and detailed fashion than what was available only a few short years ago. So how should researchers address these new circumstances in going about their scientific inquiries? And what of this is private?

PRIVACY UNDER THE U.S. CONSTITUTION AND THE LAW

Exactly where to draw the line with regard to protected privacy is not always obvious, and has shifted with the advent of various technologies. Five U.S. Supreme Court decisions turning on the use of technologically generated information occurring over the last century demonstrate this reality. The basis for the legal conception of privacy in the United States goes back even further to the U.S. Constitution at the end of the eighteenth century, in particular, to the 4th Amendment:

> The right of the people to be secure in their person, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue but upon probable cause supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (U.S. Constitution, Amendment IV 1791).

Arguments based on a right to privacy predominantly appeal to the Fourth Amendment, although it should be noted that the word *privacy* does not appear in it or the rest of the Constitution. This is especially telling for those legal scholars who debate about originalism versus interpreting the U.S. Constitution as a living document, since none of the information technologies at the center of the following cases existed when the Founding Framers wrote the Amendment. The legal opinions in these cases reflect the challenges of trying to interpret the concept of privacy in the context of new information technologies, and the lack of a clear consensus about when the government has crossed the line.

Olmstead v. United States (1928)

The information technology at issue in *Olmstead v. United States* was the tapping of a landline between telephones connecting the homes and businesses of a bootlegging organization during Prohibition. Olmstead appealed the guilty verdict, claiming that the wiretapped information was a violation of the right to privacy under the 4th Amendment.

In the majority opinion, Justice Taft rejected the appeal, stating that there was no violation of the Fourth Amendment, because the wiretaps were placed on the telephone lines in between the bootleggers' homes and businesses, not inside them (Olmstead v. U.S. 1928). He distinguished between access to the content of telephone conversations and to the contents of sealed letters which could be transported by carriers from person to person, which he considered private.

In his dissent, Justice Brandeis gave expression to a right to privacy which he saw embedded in the Constitution and was violated in the case:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect…They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone – the most comprehensive of rights, and the right most valued by civilized men (Olmsead v. U.S. 1928, 479).

Brandeis declared that the Court must extend the application of the Constitution to objects coming into being that the Framers were unaware of, and asserted that the private nature of the content of telephone conversations was equivalent to the private nature of the content of private letters.

Brandeis had already expressed his concerns about the protection of privacy before he reached the Supreme Court Bench. In a Harvard Law Review article he wrote with Samuel Warren, they deplored the existence of two emerging popular phenomena: One was the newspaper enterprise, which bolstered the public appetite for titillating or scandalous information by publishing intrusive stories about the private lives of celebrities and public figures; the second was the technological development of instantaneous photography, which meant that the press no longer needed to gain the cooperation of society figures moving about in public to take pictures of them to accompany their scandalous news stories (Warren 1890, 193-220). They considered these developments to have an adverse impact on people's "right to be let alone".

Katz v. United States (1967)

The information technology at issue in *Katz v. United States* was a listening device attached to the outside of a telephone booth Katz used to receive gambling bets. Katz's attorneys argued that this was a violation of the 4Th Amendment. A lower court had found that since there was no physical entry into the phone booth, there was no 4th Amendment violation.

In the majority opinion for the Supreme Court, Justice Stewart found that bugging the telephone booth was indeed a search and seizure violating the 4Th Amendment, and the evidence was dismissed (Katz v. U.S. 1967). The Olmstead decision was overturned with respect to the idea that a physical invasion must take place in order for the 4th Amendment to be violated; rather, the Court found that the Amendment's purpose is to protect people, not spaces.

Justice Harlan wrote a concurring opinion identifying a standard or test for determining whether the right to privacy has been violated. Harlan wrote that "…there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy, and second, that the expectation be one society is prepared to recognize as 'reasonable' (Katz v. U.S. 1967). This became known as the Katz test.

In his minority dissent, Justice Black argued for the more traditional position that there was no violation of the 4Th Amendment, because the 4th Amendment requires a physical invasion and the taking of something tangible, and no such invasion or taking occurred. He argued that the Court's opinion represented a re-writing of the 4th Amendment, which the Court was not entitled to do. As he declared:

> The Court talks about a constitutional "right to privacy" as though there is some constitutional provision or provisions forbidding any law ever to be passed which might abridge the "privacy" of individuals. But there is not. (Katz v. U.S. 1967)

Smith v. Maryland (1979)

The information technology at issue in *Smith v. Maryland* was a pen register used by the telephone company to record the landline calls made by Smith to his burglary victim to further harass her in her Baltimore home. Smith argued that the telephone numbers recorded by the pen register were protected under the 4th Amendment.

Applying the standard developed by Justice Harlan in Katz, Justice Blackmun wrote the Court's opinion finding that the third party telephone company's re-disclosure of Smith's having given the number to the telephone company in the process of making the calls was not protected information, because Smith did not have a legitimate expectation of privacy with regards to the telephone numbers he gave to the telephone company (Smith v. Maryland 1979). Smith had assumed the risk of giving the numbers to a 3rd party, namely, the telephone company.

In a dissent, Justice Stewart (with Justice Brennan's concurrence) asserted that the numbers were protected by the 4th Amendment, and that the Katz standard was satisfied. In another dissent, Justice Marshall (with Brennan's concurrence) argued that the information should have been protected, because the purpose of the disclosure of the information to law enforcement was different from Smith's purpose in giving the number to the telephone company for the limited purpose of making it possible to place the calls. Marshall also declared that the option of not assuming the risk of giving out the numbers by not using the telephone was not a realistic alternative. And both dissents raised the specter of the government's intruding on the public's privacy by circumventing the 4th Amendment's protections by simply announcing that it would monitor first class mail and telephone conversations and thereby destroy any reasonable expectation of privacy, which they contended would be extremely disturbing public policy.

United States v. Jones (2012)

The information technology at issue in *United States v. Jones* was a global positioning system (GPS) tracking device surreptitiously placed on the bottom of a Jeep Cherokee to generate evidence of Jones' use of the Cherokee to travel to places consistent with the operations of a cocaine trafficking ring. At trial, Jones argued that the use of the GPS tracker was a violation of his 4th Amendment rights.

In the majority opinion, Justice Scalia found that Jones' 4th Amendment rights were indeed violated (U.S. v. Jones 2012). Scalia noted that the tracker on the Cherokee was an instance of an unreasonable physical search of an "effect" (the Cherokee) as mentioned in the 4th Amendment. He also dismissed the Katz test.

Justice Sotomayor concurred with the Court's opinion that the 4th Amendment had been violated, and pointed out that people constantly show themselves to other people in the course of ordinary daily life. She opined that disclosure to a third party for a limited purpose may still deserve the protection of the 4th Amendment. Justice Alito also concurred, and declared that the issue of physical intrusion in this case was not important; rather, the violation of the 4th Amendment was due to the collection of information through the lengthy monitoring of Jones' behavior. And he pointed out that with technological change may come changes in what society views as a reasonable expectation of privacy.

Carpenter v. United States (2018)

The information technology at issue in Carpenter v. United States was cell-site location data obtained from wireless carriers to show that Carpenter's cell phone pinged off of radio antenna cell sites near four robbery sites coinciding with the times of those robberies. Carpenter argued that the use of this information to prosecute him was a violation of his 4th Amendment rights.

In his majority opinion, Justice Roberts declared that Carpenter's 4th Amendment rights were violated, using the Katz/Smith test, saying that the volume of information obtained was unique and sufficient to make it a search violating a reasonable expectation of privacy in Carpenter's physical movements over a long period of time (Carpenter v. U.S 2018). Appealing to Brandeis's dissent in Olmstead v. the United States, he argued that the Court needs to keep "the progress of science" from eroding 4th Amendment protections.

In dissent, Justice Kennedy wrote that 3rd party records are not protected by the 4th Amendment, and so there was no search of Carpenter. Some businesses are not bailees or custodians of the customer records they hold, with a duty to hold them for the customers' use.

Justice Thomas also dissented, saying that there was no 4th Amendment violation, because Carpenter's property was not searched. He also asserted that "[t]he Katz test has no basis in the text or history of the Fourth Amendment" (Carpenter v. U.S 2012, 2).

Justice Alito wrote a dissent pointing out that the Court opinion ignored the issue of 3rd party holders of data, and distinguished between a search and a compulsory process of obtaining information, only the former of which he thought was covered by the 4th Amendment. He suggested that the Katz test serves to extend rights beyond those of property law, to information held by third parties who may be bound not to disclose that information. He argued that legislation should be the appropriate instrument for protecting such information, not the 4th Amendment.

Justice Gorsuch, in his dissent, suggested using the property-based interpretation of the 4th Amendment for upholding protections against searches of someone's papers and effects does not necessarily imply that they disappear because people share the papers or effects with third parties. Persons may have a property interest in things they have given to third parties, but this would not be an argument based on the Katz reasonable expectation of privacy test. *Bailments* involve a person giving someone else their personal property for a certain purpose. A bailee who uses the item in a different way than they are supposed to according to the conditions of the transfer is

liable for theft. Gorsuch did not reject the Katz test outright, but suggested that a property-based approach to interest in third party information is more appealing.

Several important points emerge from this set of cases. All of them involve the use of information technologies which made the generation and preservation of information possible and that did not exist when the U.S. Constitution and Bill of Rights were written. In three of the cases, the agents collecting the information obtained it directly from the individuals themselves, by using devices that enabled them to observe the individuals who were unaware of being observed and clearly meant to keep the information to themselves. In the other two cases the information was recorded by a third party, and the law enforcement agents obtained the information from the third party. Both the content of the information, and the quantity of information, could be relevant to a determination of a violation of privacy. Where the individuals were providing information to a third party, their purpose in providing the information, what the third party might do with their information besides the original purpose for which it was given, whether the originating individuals retained any property or other rights with regard to the information conveyed, whether the third party was under any constraints with regard to what they may do with the information, and even whether the originating individuals were aware of the information uses of the third party, are all relevant considerations.

The opinions voiced in these legal cases suggest that it is important to distinguish between information obtained through the observations of individuals themselves and information generated or obtained by third parties about individuals. This distinction roughly parallels the Common Rule's two criteria for what is considered "private information". In the following, we will consider 'privacy' to include the first criterion but not the second; 'privacy' means the condition or state of being secluded from others or observation. The personal information given over to or generated by third parties referred to in the second criterion should not be considered 'private', for the purposes of the Common Rule, even though the Common Rule should still be used to protect the people to whom it refers.

THE PRIVATE, THE PUBLIC, AND THE SOCIAL

The traditional construction of private and public as exhaustive binary terms is inadequate to the task of exhausting the possible options for the kinds of personal information available to researchers. Much of the personal information researchers want to use is neither wholly public nor private, but rather sits somewhere in between. It is not fully public because there are some constraints on how that information may be accessed, used, and passed on, which arguably makes such information confidential to some degree. But the conditions attached to the access and use of that information should not be the same conditions as those that should be attached to what is entirely private, where the individual normally has exclusive control over disclosures of the information. An approach incorporating the intermediate status of third party-held personal information would make it easier to understand how to properly access and use the information lying somewhere between the public and the private, and perhaps provide a clearer picture of when stricter dictates of privacy should be adhered to.

The evolution of information technology has increased and widened the kinds of information about individuals held by third parties who are bound to limit disclosure of that information. These third parties have their own interest in the information they have such that the individuals the information is about do not and should not have exclusive control over it. Banks need to know about their customers' accounts in order to serve their clients and make reasonable decisions about their investments; school systems need student information in order to evaluate their teaching and learning programs and certify student attainment and achievement; businesses need personnel records to oversee their employees; clinical care providers need patient medical records to make clinical care decisions, do quality assurance and improvement, and carry out insurance and billing processes. Etc. What the third parties can do with the personal information they have, who they can disclose it to, and under what conditions

should depend on the kind of information, the terms under which the information was given over, and the purposes of the relationships they have with the individuals whose information they hold.

Arendt maintained that the problem of sorting out the public and the private has been building for centuries. Long ago, many of the ordinary activities of daily life took place within the household, shielded from public view. But as time went on, many of these activities moved out of the household into various social locations, and consequently the information about them has also become more widely accessible:

> The emergence of society – the rise of housekeeping, its activities, problems, and organizational devices – from the shadowy interior of the household into the light of the public sphere has not only blurred the borderline between private and political, it has also changed almost beyond recognition the meaning of the terms and their significance for the life of the individual and the citizen (Arendt 1958, 38).

Following Arendt's designation of this realm of human life as being social, we will label the information held by third parties that is neither fully public nor private *social*; and to remind ourselves that this social information is not public because there are limitations or conditions attached to the access and use of this information which distinguish it from fully public information, we will refer to it as *restricted social information (RSI)*.

RSI would include information generated and maintained by third parties in various social contexts. Medical, school, bank, business personnel, commercial transaction, classified information, and government-controlled correspondence records would fall within this realm. So would information stored from the activities of online shopping and internet use with service providers and website use covered by end user license agreements or terms of service or privacy agreements.

On this view, *privacy* refers to the condition or state of being secluded from others or observation. Private information is information whose sources are homes, diaries, journals, personal computer files, other personal physical records, and individuals themselves. *Public* refers to what is open and accessible to anyone in the community or society, without restriction. Public information's sources are streets, stadiums, theaters, stores, public libraries, magazines and newspapers, radio and television, Twitter, Instagram, and other open access online media.

Parallel to the recognition of RSI is the recognition of information derived directly from observation of individual behavior that is neither public nor private. Behavior occurs in all kinds of circumstances where access is controlled to some degree, and yet the conduct of the individuals who interact in those circumstances is not limited or controlled by any one individual. These circumstances include school classrooms, clinical care facilities, many business and commercial workplaces not open to the public without permission, some religious practices, and much of the activity in government offices. Online, interactions on platforms such as restricted access chatrooms that are limited or controlled in some way are also neither public nor private. Such behavior will be called *restricted access social behavior* (RASB). Obviously RASB is also of interest to the research community. RSI and RASB both exist between the private and the public spheres.

INCORPORATING RSI AND RASB INTO THE COMMON RULE

The recognition of RSI and RASB would require regulatory revisions to the Common Rule. The current second descriptor of private information, namely "…information that has been provided for specific purposes by an individual and that the individual can reasonably expect will not be made public (e.g., a medical record)" would need to be removed as referring to private information, because this is what RSI refers to. The question then becomes how the regulations should apply to research involving RSI and RASB.

The Common Rule could be revised to completely exclude research involving only RSI. The description of private information would be revised to refer to information obtained from individuals themselves or generated through intervention, interaction, or observation of them. Investigators conducting research using RSI would only

need to abide by whatever conditions are attached to getting access to the RSI in question, as reflected in other laws, regulations, policies, agreements, terms and conditions. From a regulatory standpoint, the issue of the identifiability of RSI would be moot, because even if the information were identifiable, it would not be "identifiable *private* information". There would no longer be requirements for informed consent (or waiver of informed consent) and institutional review board (IRB) approval of such research under the Common Rule. IRBs would be relieved of the burden of reviewing such research projects, including the need to be familiar with the conditions attached to the access and use of the specific kinds of RSI under consideration. IRBs could then devote more of their time and attention to research projects that involve direct interventions, interactions, or intrusions in the lives of individuals themselves, which arguably pose higher risks. Policymakers who are sympathetic to the idea of de-regulation may find this option appealing.

The problem with this approach is that it does not provide adequate protection for the research subjects of RSI. Researchers at research institutions are not always familiar with the legal and ethical responsibilities of accessing and using the myriad varieties of RSI, and Common Rule oversight mechanisms can provide that assistance where needed. A seasoned researcher much of whose career has been dedicated to secondary research studies in particular areas may well know what requirements they need to satisfy in order to access and use RSI to do their research studies responsibly. Novice researchers, however, or researchers seeking to expand or shift to a different source of information they want to make use of, may not have that familiarity. The conditions attached to different types of RSI vary in how difficult they are to understand and fulfill, and in some cases while the third party holders of the RSI are well protected by the existing mechanisms for use and disclosure, the subjects may not be. One violation of the terms and conditions of research access and use of RSI, or a failure to provide appropriate confidentiality of RSI, can substantially damage the research institution's reputation for its research, and trust in the institution may be difficult to restore. A research institution's human research protection program may serve as an important resource in this regard.

Research involving only RSI could be reviewed according to three alternative different processes under the Common Rule: 1) The research could be reviewed and approved by the convened IRB with all of the relevant requirements of the Common Rule; 2) the research could be reviewed and approved through the expedited review process, using the same approval criteria as convened IRB approval; or 3) a new category of exempt research could be created according to which IRB approval would only require adequate protection of the confidentiality of the information and the use of the information consistent with the conditions of the particular restriction terms to which the data are subject. This latter would seem to be the most appropriate mechanism for most research uses of RSI, since presumably the RSI's terms should stipulate appropriate conditions attached to that data, and the IRB could still invoke appropriate confidentiality safeguards if the RSI's disclosure conditions are lacking. This approach would represent a reduction in the administrative burdens associated with RSI, while still providing appropriate human subject protection.

The insertion of the social between the public and the private also raises the issue of whether researchers investigating restricted access social behavior (RASB) should fall under the Common Rule. If researchers intervene or interact with subjects in venues where access is restricted, the Common Rule as currently written should apply unless exempt, regardless of whether the information obtained is private, restricted, or public. The circumstances of research involving RASB deserve particular scrutiny, since the impact of the institution restricting the individuals' behavior should be taken into account in assessing the adequacy of the subjects' protections, and the IRB should also be mindful of whether the restricting institution is entitled to set any conditions on the research.

Some RASB research could be conducted without any intervention or interaction with subjects. Ethnographers doing qualitative research studies of behavior in restricted settings may gather information through passive surveillance of social interactions, such as simply observing behavior in restricted physical settings or online by lurking or otherwise surveilling behavior without intervening or interacting with subjects. Here again, technological innovations could make observation possible without intervention, interaction, or even subject

awareness.[1] The issues are complicated here, both with respect to the subjects themselves and with the institutions within which the observation occurs. Subjects may deserve to be notified, or even have the discretion to consent or decline to participate in such research. And the institutions restricting access to these social spaces may also be entitled to have a say in whether such research may occur. Common Rule oversight is called for in such research. The expedited review procedure may be appropriate in some cases.

The following three examples illustrate some of the complexities of research management of restricted social information often sought by researchers.

The *Health Insurance Privacy and Portability Act (HIPAA)* and its attendant regulations provide for research access to electronic health record information held by the institutions under its jurisdiction (Health Information Portability and Privacy Act of 1996, 42 U.S.C. §1320d et al. and 45 C.F.R. §160 and 164, 1996). The institutions, not the patients themselves, hold these data, and there are a number of provisions for appropriate disclosures of the information regardless of the wishes of those patients, e.g. reporting gunshot wounds to public authorities. HIPAA countenances both research with de-identified data and research with identified data. HIPAA's regulations both allow for research access to the data with patient permission or under a waiver of authorization for the patients involved, and provide appropriate confidentiality protections for research uses of the record data.

The 2018 revised requirements of the Common Rule defer to the HIPAA protections for secondary research of this kind. In other words, the federal regulations exempt secondary research protected under HIPAA from the Common Rule such that IRB approval is not required, based on the presumption that the HIPAA protections are sufficient. This approach is consistent with this essay's general proposal for the regulatory approach to research studies with RSI.

The *Family Educational Rights and Privacy Act (FERPA)* and its attendant regulations provide for access to information in student education records if specified conditions are met (Family Educational Rights and Privacy Act of 1974 20 U.S.C. § 1232g and 34 C.F.R. § 99, 1974). FERPA protects education records about students that are held by education agencies, such as schools, and thus clearly apply to education agencies as third parties. (FERPA does not apply to information held by the students themselves.) Parents are explicitly given certain rights with respect to those records (e.g. the right to inspect and seek to correct education records). Research access to education records without parental consent (or student permission upon the age of majority) is allowed if "…The disclosure is to organizations conducting studies for, or on behalf of, educational agencies or institutions to: (A) Develop, validate, or administer predictive tests; (B) Administer student aid programs; or (C) Improve instruction" (Family Educational Rights and Privacy Act of 1974 20 U.S.C. § 1232g and 34 C.F.R. § 99.31(a)(6)(i)). If a researcher wishes to obtain student education record data for a research objective that does not fall under one of these categories, the researcher would need to obtain parental consent in order to access and use the data.

FERPA illustrates the challenges of properly following and interpreting regulations: First, what counts as "improving instruction"? For example, if a researcher is simply comparing student gender and academic achievement, is this conducting research to improve instruction? And second, the FERPA provision for research without parental consent is conditioned on the destruction of the data when the data are "… no longer needed for the purposes for which the study was conducted" (Family Educational Rights and Privacy Act of 1974 20 U.S.C. § 1232g and 34 C.F.R. § 99.31(a)(6)(iii)(B)); such destruction is not typically standard research practice, and researchers unaware of the provision may unknowingly violate it by retaining the data for other future research purposes.

The *Protection of Pupil Rights Amendment (PPRA)* and its attendant regulations permit the conduct of evaluations in which students are asked to disclose information in any of eight sensitive categories of information, with parental consent or notice and the opportunity to opt out, where the evaluation occurs at educational institutions

[1] Because 'intervention' and 'interaction' are also described in the Common Rule in open-ended fashion, it is possible that the Common Rule could be interpreted to preclude any collection of information directly from subjects as not involving intervention or interaction, but this interpretation would be difficult to defend.

receiving funds from the U.S. Department of Education (Protection of Pupil Rights Amendment 20 U.S.C. §1232h and 34 C.F.R. § 98 (2001)). (Nearly all public schools in the United States receive such funding.) Complying with PPRA is challenging for researchers in several respects: First, since PPRA applies to evaluations of students, a researcher actually conducting such an evaluation is interacting with students and obtaining information about them. So the Common Rule would likely apply to the primary study activity. Alternatively, if the researcher is seeking information from education agencies who collected it under separate student evaluation activities, then the researcher is seeking RSI from the education agencies, which would mean that while the information is not private, the researcher must still comply with the requirements of PPRA. What is considered consent or parental permission or parental notice and the opportunity to opt out under PPRA is not the same as informed consent under the Common Rule. And if the evaluation itself was funded by the U.S. Department of Education, the parental permission or notice requirements are different from those if the funding came from elsewhere. Further complicating matters, the PPRA regulations have not been revised since the last revision of the PPRA statute itself, which included, for example, adding an additional category of sensitive information pertaining to "… religious practices, affiliations, or beliefs of the student or student's parent" (Protection of Pupil Rights Amendment 20 U.S.C. §1232h). PPRA already contained a category about "sex behavior and attitudes". Whether information sought pertains to religious beliefs, or to sex behavior and attitudes, is not always obvious. The U.S. Department of Education's Family Privacy Policy Office provides some general guidance about how to apply some provisions of PPRA, (U.S. Department of Education) but significant questions about how to interpret the law, without up-to-date regulations, remain unanswered.

If the category of RSI were to be incorporated into the Common Rule, the Common Rule's requirements for research involving RSI could be used to apply to these specific kinds of studies. By revising the current exemption for some secondary research studies, the Common Rule could exempt any research study of RSI, provided that the study complied with the Common Rule's requirements for limited IRB review of the confidentiality protections for the study, (HHS 45 C.F.R. § 46.104(d)(7) and.111(a)(7)) and the study's compliance with any other laws, regulations, policies, agreements, or terms and conditions applicable to the RSI involved. This would relieve the study of the other requirements for the approval of research under the Common Rule, but still retain IRB oversight responsibility for ascertaining the adequacy of the data confidentiality protections and for compliance with other requirements such as the PPRA's parental notice and permission requirements..

Inserting provisions regarding research involving RSI or RASB into the Common Rule as proposed would result in the following revisions:

Definitions:

Human subject means a living individual about whom an investigator (whether professional or student) conducting research:

> (i) Obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or
>
> (ii) Obtains, uses, studies, analyzes, or generates identifiable private information, identifiable *restricted social information*, or identifiable biospecimens [italics added]
>
> Identifiable *restricted social information* is individually identifiable information that is held by a third party and may only be released to investigators according to any applicable formal policy such as a law, regulation, electronic user license agreement, or terms of privacy.

In addition, the Common Rule's exemption categories for secondary research studies would need to be revised to address secondary research studies involving RSI.

ADDRESSING PRIVACY

Incorporating the concept of RSI into the Common Rule is only a partial solution to appropriately revising the function of the concept of privacy in the Common Rule. Having argued that a considerable portion of the information that is currently labeled 'private' is not really private and shouldn't be considered so, this brings us back to the question of what is genuinely private information. If the research regulations were revised to separate RSI from information that should be considered truly private, the task remains of identifying what should be considered private, and how researchers should approach gaining access to it. There is more to the protection of privacy in research that needs to be sorted out.

In Brandeis' famous dissent, he refers to "…beliefs, …thoughts, …emotions and … sensations…", as elements of people's "spiritual life". The strength of this appeal depends at least in part on the reality that these are perhaps the innermost features of human life, and that if these things are not private, nothing could be. But Brandeis was also clearly concerned about shielding individual phenomena that can be directly observed, but which ought not be observed and revealed, because getting access to them may create unwanted inroads into people's spiritual lives. His law review article is directed primarily at the intrusiveness of the media into people's personal lives as a threat to privacy.

Unlike the regulatory research community, which has primarily focused on modernizing the approach to the identifiability of personal data, other scholarship has examined the idea of privacy and how the evolution of information technology has forced us to re-examine its nature, value, and protection. Some scholars favor resorting to other means to address the concerns about how to regulate access to personal information, because the idea of privacy is so perplexing, while others continue to make use of privacy to safeguard certain features of human life. The concept remains elusive, but some of this work is quite insightful.

In her philosophical analysis of the several areas of human life, Arendt distinguished between the public and the private realms, and suggested that "„„[t]he most elementary meaning of the two realms indicates that there are things that need to be hidden and others that need to be displayed publicly if they are to exist at all" (Arendt 1958, 73). She offered as examples of what is naturally hidden the phenomenon of pain, the activity of thinking as the love of the reflective activity of pursuing wisdom, and the exercise of goodness as represented in the teachings of Jesus of Nazareth. Her examples parallel Brandeis' references to various elements of spiritual life, but again there is the notion that not just what is actually interior to people's spiritual lives, but also some physically observable things, such as feelings and thoughts people put on paper or other media, or actions which people take in certain contexts, which reflect their spiritual lives and the aspects of their existence that may flourish only in solitude or in settings absent others' observation. Arendt was pleading for the recognition of the importance of the private dimension of human life, but did not directly address mechanisms to protect it.

More recently, Helen Nissenbaum has recognized the inadequacy of the public/private information distinction as a workable approach to determining what personal information can and should be disclosed or protected in the plethora of information generated, preserved, and circulated via the various forms of evolving information technology (Nissenbaum 2010). She argues for an approach termed *contextual integrity*, in which the norms of information use governing particular domains such as medicine, education, commerce, etc. should serve to prevent people from being surprised and perturbed by information disclosures. Laws, regulations, and policies etc. should be crafted to support these norms, and may be subject to revision if the evaluation of the effects of new technologies identify flaws with regard to when and how personal information is handled in keeping with both legitimate social goals and the protection of personal expectations. This approach does not rely on any specific view of what constitutes privacy, but rather substitutes the contextual integrity approach to protecting people from objectionable disclosures of personal information about them by third parties, whatever the source.

Paul Ohm, another leading thinker in the area of information privacy in the context of evolving technology, offers an approach to information protections through his analysis of "sensitive information" and the harms that may

be associated with it (Ohm 2015). He offers an open-ended catalogue of various types of sensitive information, including health, sex, financial, personal safety, etc., and divides sensitive information into three kinds: (1) "Inherently sensitive information" which may itself cause harm simply by virtue of being known to another; (2) "inferentially sensitive information", which may cause harm because of conclusions about people that are drawn from that information; and (3)"instrumentally sensitive information", which is information that is not itself sensitive but could be used to do someone harm, e.g. the home address of someone who could be the object of a stalker. He argues that laws and regulations protecting information should be crafted to protect sensitive information so as to prevent harms. By focusing directly on the harms information may pose, Ohm's deliberately practical approach also does not need to wait for the resolution of controversies over the meaning of privacy.

As a regulatory matter, however, Nissenbaum's and Ohm's approaches do not accomplish the task of deciding how to set the parameters of the meaning of privacy in the Common Rule. Separating off RSI in the Common Rule as distinct from private information in accordance with any of the options described above does not by itself provide a solution to the problem of how to describe private information in the Common Rule in such a way as to set the boundary of what kind of research falls within the jurisdiction of the Common Rule 's protection. According to the first prong of the definition of a human subject in the Common Rule, the Common Rule applies when information is collected for research if there is any "…intervention or interaction with the individual…" regardless of whether it is private or not. But in addition to obtaining information about an individual from sources falling within the category of RSI, there remain other ways for investigators to obtain information about individuals that could well be considered private. Investigators could observe individuals and collect information about them without any intervention or interaction, and information technologies have expanded the various ways in which this is possible. Furthermore, investigators may elicit information about individuals from persons other than the individuals themselves, the nature of which is considered private, but which is not bound by any regulation, policy or agreement, but rather is the artefact of some personal relationship or association. And the provision directing the Secretary of HHS to provide guidance about the protection of privacy and the confidentiality of data also seems to imply the protection of an area of the lives of people themselves in some respect, and not just information about them.

Anita Allen argues forcefully for the importance of protecting privacy in a liberal democracy, both for its effect on the flourishing of individuals' own lives and for the well-being of the society of which they are members (Allen 2011). On her view, the common public understanding of privacy includes 1) physical privacy, 2) informational privacy, 3) decisional privacy, 4) proprietary privacy, 5) associational privacy, and 6) intellectual privacy. People need both the opportunities and the actual experiences of private life to enhance who they are and how they may engage with each other in public. Some elements of private life - she singles out informational privacy and physical privacy - are so important in her view that government should not only allow people the option of protection of their privacy in some measure, it should require them to. Government should be paternalistic in some laws requiring people to retain their privacy. Allen's argument includes, but is not limited to, the protection of personal information that dominates the current discussions of privacy and its imputed demise.

Following in the tradition of Arendt's thinking, Lowry Pressly argues for the importance of a "right to oblivion", based on the idea that the fullness of human life is to be attained in part through the freedom offered by private life (Pressly 2024). Pressly suggests that the existing concern over the protection of personal information distracts us from something even more important than the vulnerability created by the facts about who we already are. He draws our attention to the human potential to freely become ourselves in ways that depend on the capacity to pursue possibilities without having to constantly look over our shoulders to see who is watching. His view of privacy as "the right to oblivion" is based on an appeal to the inherent value of self-development of the individual, which transcends the significance of the facts about our existing selves.

Daniel Solove rejects the effort to identify the "essence" of privacy as fruitless (Solove 2008, 2025). A single definition of privacy would be too abstract to be useful in developing appropriate privacy protection policies.

He advances a pragmatic approach to privacy, in which he accepts a grouping of overlapping uses of the idea of privacy, and attempts to address how the problems threatening the several similar kinds of privacy should be addressed through protections tailored to those kinds. He offers a taxonomy of privacy, with four general categories (and sixteen subcategories) of private life: 1) information collection; 2) information processing; 3) information dissemination; and 4) invasions. The first three categories pertain to the several stages in the course of information generation and uses, while the fourth category has to do with direct intrusions on persons themselves. He rejects the idea that the protection of privacy is a cost to society, arguing that the protection of privacy is not only valuable to the individual but also to society.

In their classic bioethics textbook, Tom Beauchamp and James Childress favorably cite Allen's list of popular categories of privacy (Beauchamp & Childress 2019). They acknowledge the consequential value of privacy, in terms of how privacy may contribute to personal self-development, intimate personal relationships, and the exercise of freedom, which derive from the ethical principle of beneficence. At the same time, they suggest that the primary justification for the protection of privacy comes from the principle of respect for autonomy, the idea that people should be able to control their own lives. For the purposes of policy, instead of trying to precisely set the bounds of privacy as a whole, they recommend developing policies which identify particular zones of privacy interests, and set the conditions for how and on the basis of what interests privacy may be intruded upon.

The various theorists' defenses of privacy reflect the reality that there are multiple motivations for intruding on people's privacy and making what was private public, or at least accessing it by others, and that those motivations carry with them justifications of different kinds for intrusion: Some people may be motivated by sheer curiosity; others assert the exercise of their freedom of expression; the press wants the freedom to uncover and publish what they think the public wants to know about; public welfare agencies want to know about private attitudes, opinions and behavior so as to design policies and programs to promote various social goods, such as public health; businesses want to know what people do in private so they can market goods and services to them; and investigators have scientific questions to be answered about private human attitudes, beliefs and behavior across the spectrum of human life.

The challenges of determining what is private are manifold. Privacy varies across culture; what is private at one time and in one culture may not be so in another (Hawkins 2024). Privacy is not static; the boundaries of what is considered private may shift over time within a culture. Privacy can be relinquished: if someone chooses not to exercise their right to privacy, e.g. the public disclosure of a medical condition, this is not a violation of privacy. So the nature of the information itself is not sufficient to determine whether or not one's privacy has been violated. And technological advances have altered what can reasonably be considered private, both by generating private information that could not exist before the technological mechanism became available, and by facilitating the ability to observe formerly private behavior or readily gain access to guarded information.

Privacy has to do with being free from intrusion or observation by others, as Brandeis put it, to being "let alone". People do all kinds of things in private, from meditating to reading to sex to exercise to playing to eating to sleeping to substance use to self-abuse to other-abuse. Or they may do nothing at all. Some of this is good, some of it is bad, and some of it does not matter. The importance of privacy at any given moment will vary with how people are using it; consequently, the significance of not intruding on their privacy will vary as well. However, depending on the method through which their privacy is observed or invaded, the significance of the infringement may only be discovered after the fact. And the exercise of one's privacy often depends on having the confidence that there will be no infringement on that private time, irrespective of how it is spent.

If researchers wish to inquire into what is private in this sense, a different set of considerations than those associated with RSI would seem to apply. Unlike the exploration of the various types of RSI by researchers to investigate whatever scientific question they might wish to pursue, research inquiry into the truly private threatens the vitality of the very phenomena it seeks to understand. Observation may itself distort, damage, or destroy what it looks at, regardless of whether what is observed is secondarily disclosed or used in any way. (This is not the case

with at least a large portion of secondary analyses of RSI, so long as the confidentiality provisions are effective; this information remains intact, and can be generated and used by others for specific legitimate purposes.)

A special onus is therefore on the researcher to justify any intrusion into the genuinely private. It may be that the preciousness and fragility of some dimension of the private is such that researchers are bound to leave it alone, even if it means forgoing the answer to a legitimate scientific question. Simple intellectual curiosity may be insufficient as a justification, or even some findings that may shed light on a significant social issue or problem. On this view, sometimes people should just be left alone.

For some research questions exploring what is private, individual consent of the subject may be a legitimate way to open the door to research inquiry. People are not always obliged to keep everything private, and so obtaining information about people's private lives may be ethically defensible under condition of their informed consent. If the impact of research observation of the quality of their otherwise private lives is acceptable to them, people may allow researchers to be an audience. Without such consent, however, researchers may be ethically obliged to look away.

The Common Rule includes a condition in its provision for waiver of informed consent stipulating that the waiver should not adversely impact the rights and welfare of the subjects. This regulatory condition cannot logically refer to the right to informed consent to research itself, because then the condition would never be satisfied by the waiver. But here a right to privacy or oblivion could represent a distinct right that is not identical to the right to consent to research; it could be that the right to privacy prohibits the waiver of consent for seeking some kinds of information in some ways. It could also be true that the welfare of subjects could be jeopardized by the possibility that researchers might seek to observe and obtain certain private information about them without their consent, but not always. And the same could be said with regard to intervening or interacting in people's private lives. The justification for doing so would depend on the specific nature of the private phenomena, and the specific research inquiry.

In view of the diversity in the mentioned and other leading theoretical approaches to privacy, and the apparent abstract complexity of the concept, it seems inadvisable to introduce a specific elaborate and detailed conception of privacy into the Common Rule that is driven by one contending theory as distinct from the others. On the other hand, it is also apparent that some indication of what privacy is needs to be provided to identify the broad parameters of when privacy concerns should be considered.

The introduction of RSI would provide some guidance with respect to how third party information that is confidential should be managed, separate from the approach to privacy itself. Appropriately addressing the confidentiality protections of RSI in its diverse forms is largely separable from the issues of protecting the privacy of individuals themselves. The guidance that the Secretary of HHS is supposed to issue could clarify the ways of protecting confidentiality, and the separate topic of what privacy is and how to protect it.

Privacy refers to the condition of being secluded from society or the public. The Common Rule could be revised to include this general umbrella idea, along with a reference to the most salient categories of personal privacy which this idea includes. It would probably be unwise to make that list exhaustive, to present a fixed exclusive definition of privacy. This approach would identify some regulatory basis to the research community and IRBs about how to understand what should be protected under the Rule, but still provide a measure of flexibility to allow for appropriate interpretation of the Rule in specific cases, some of which will be unusual. Federal agencies such as the Office for Human Research Protections could issue guidance giving additional advice about how to apply the regulatory provisions in the kinds of research studies conducted or supported by the Department of Health and Human Services to studies of various kinds of privacy.

The current language in the Common Rule refers to "…information that occurs in a context in which an individual can expect that no observation or recording is taking place…", echoing the language of the first prong of the Katz test. But it says nothing about what those contexts might be. The Common Rule should do more than that. The Common Rule could include something like the following:

> *Privacy* refers to the conditions in which individuals are normally secluded from the rest of society, including their physical selves, personal records, places such as the home, intimate relationships with others, their solitary behavior, and their spiritual lives. *Private information* is information about these aspects of their lives.

CONCLUSION

The first purpose of this essay is to argue that there is a considerable corpus of nonpublic identifiable personal information controlled and disclosable by third parties that should not be interpreted and treated as "private" under the Common Rule. This information is or perhaps should be protected by law, regulation, policy, or formal agreement. Existing laws, regulations and policies do well or not so well at providing appropriate levels and mechanisms of protection. Researchers should be aware of and abide by the provisions of those rules, and sensitive to their limitations. Human research protection programs at research institutions should have ways of encouraging and ensuring that researchers are aware of and follow those rules. The Common Rule could be revised to apply to specified types of RSI as being within its scope of its jurisdiction, as warranted. One option would be to create an exemption for research using RSI, if the research is approved via limited IRB review for protection of the confidentiality of the information and consistent with the third party's conditions for use and disclosure. This exemption could apply to all RSI, or it could be crafted to apply to specified categories of RSI.

Second, this essay also points to the importance of preserving a distinct approach to research about what is genuinely private. It does not propose a completely definitive specification of the private that fully clarifies the nature and scope of privacy, but it goes some way toward identifying how privacy could be characterized in the Common Rule for the purposes of the research regulatory community. Legal theories about privacy continue to evolve, rival views about the nature of privacy are actively supported, and arguably a comprehensive theory of privacy in the modern technological context has yet to be developed. But for the purposes of research inquiry into what is private, the general idea that privacy pertains to whatever about a person is meant not to be observed or intruded upon in some ways without compelling justification provides some guidance, and is distinct from RSI. The historical and cultural variation in what has been treated as private implies that there ought to be some flexibility to the term, but that does not make it meaningless. Research observers should be especially careful about whether to try to observe or inquire into what is meant not to be seen.

REFERENCES

Acquisti, Alessandro, Laura Brandimarte, and George Lowenstein. 2015. "Privacy and human behavior in the age of information", in *Science,* Vol 347, Issue 6221, (January 30, 2015): at 509-514. doi: 10.1126/science.aaa1465

Allen, Anita L.. 2019. "The Philosophy of Privacy and Digital Life", APA presidential address, (93) *Proceedings of the American Philosophical Association,* at 21-38.

Allen, Anita L. 2011. *Unpopular Privacy: What Must We Hide?* Oxford University Press.

Arendt, Hannah. 1958. *The Human Condition*. University of Chicago Press.

Arendt, Hannah. 1970. *On Violence*. Harcourt.

Beauchamp, Tom A. and James F. Childress. 2019. *Principles of Biomedical Ethics,* - Eighth Edition. Oxford University Press.

Carpenter v. United States, 585 U.S. 296 (2018)

Family Educational Rights and Privacy Act of 1974. 20 U.S.C. § 1232g and 34 C.F.R. § 99 (1974).

Hawkins, Simon, 2024. "What's So Special About Private Parts? How Anthropology Questions the Public–Private Dichotomy", in Mary C. Lacity and Lynda Coon, (eds.) *Human Privacy in Virtual and Physical Worlds: Multidisciplinary Perspectives*, Springer Nature: at 47-68 https://doi.org/10.1007/978-3-031-51063-2

Health Information Portability and Privacy Act of 1996 42 U.S.C. § 1320d et al. and 45 C.F.R. § 160 and 164 (1996)

Holland, Norman. 1996. "The Internet Regression", in *The Psychology of Cyberspace,* ed. John Suler (1996): https://www.psicopolis.com/psicopedia/Psychology%20of%20Cyberspace/psycyber/holland.html

Jasser, Jasser, Ivan Garibay, Steve Scheinert & Alexander V. Mantzaris. 2022. "Controversial information spreads faster and further than non-controversial information in Reddit", *Journal of Computational Social Science* no.5:111-122. https://doi.org/10.1007/s42001-021-00121-z

Katz v. United States, 389 U.S. 347 (1967)

Kramer, Adam. D., Jamie E. Guillory& Jeffrey T. Hancock. 2014. "Experimental evidence of massive-scale emotional contagion through social networks", in *Proceedings of the National Academy of Sciences*, vol. 111, No. 24 (June 17, 2014) at 8788-8790. https://doi.org/10.1073/pnas.1320040111

Li, Yao. 2022. "Cross-Cultural Privacy Differences", in *Modern Socio-Technical Perspectives on Privacy,* ed. Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, et. al. (Springer, 2022): at 267-291. https://doi.org/10.1007/978-3-030-82786-1;

Mason, Sharon. 2024. "Exploring Privacy from a Philosophical Perspective: Conceptual and Normative Dimensions," in *Human Privacy in Virtual and Physical Worlds: Multidisciplinary Perspectives,* ed. Mary C. Lacity and Lynda Coon, (Springer Nature, 2024): at 23-45 https://doi.org/10.1007/978-3-031-51063-2 ;

Murthy, Vivek. 2023. *Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory,* (Office of the Surgeon General (OSG) Washington (DC): US Department of Health and Human Services. https://www.ncbi.nlm.nih.gov/books/NBK594761/

Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford University Press.

Ohm, Paul, 2015. "Sensitive Information", in *Southern California Law Review*, Vol. 88 :1125-1196.

Olmstead v. United States, 277 U.S. 438 (1928)

Pressly, Lowery, 2024. *The Right to Oblivion: Privacy and the Good Life.* Harvard University Press.

Protection of Pupil Rights Amendment 20 U.S.C. §1232h and 34 C.F.R. § 98 (2001)

Smith v. Maryland, 442 U.S. 735 (1979)

Solove, Daniel J. 2008. *Understanding Privacy.* Harvard University Press.

Solove, Daniel J. 2025. *On Privacy and Technology*, Oxford University Press.

Suler, John 2004. "The Online Disinhibition Effect", *Cyberpsychology and Behavior* Vol. 7 No. 3 (2004): at 321-326. DOI:10.1089/1094931041291295

U.S. Department of Education, https://studentprivacy.ed.gov/content/ppra.

U.S Department of Health and Human Services (HHS). 2017. Subpart A – Basic HHS Policy for Protection of Human Subjects, 45 Code of Federal Regulations C.F.R. § 46, 82 Federal Register 7259, 7273, January 2017, as amended at 83 FR 28518, June 19, 2018, available at https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-A/part-46.

United States Constitution, Fourth Amendment (1791)

United States v. Jones, 565 U.S. 400 (2012)

Warren, Samuel D. and Lewis D. Brandeis. 1890. "The Right to Privacy", in *Harvard Law Review*, Vol. IV, No. 5 (December 15, 1890) at 193-220. http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C

Wisniewski, Pamela J. and and Xinru Page. 2022. "Privacy Theories and Frameworks" in *Modern Socio-Technical Perspectives on Privacy*, ed. Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, et. al. Springer,: at 15-41. https://doi.org/10.1007/978-3-030-82786-1