Yale Journal of Law and Technology

Volume 15
Issue 1 *Yale Journal of Law and Technology*

Article 1

2013

Moving from Nixon to NASA: Privacy's Second Strand--A Right to Informational Privacy

Christina P. Moniodis
Yale Law School

MOVING FROM *NIXON* TO *NASA*: PRIVACY'S SECOND STRAND—A RIGHT TO INFORMATIONAL PRIVACY

Christina P. Moniodis*

15 YALE J.L. & TECH. 139 (2012)

ABSTRACT

The Supreme Court's data privacy jurisprudence consists of only two cases, yet these cases have fueled a circuit split on data privacy rights. The Court's hesitance to foray into data privacy law may be because the nonrival, invisible, and recombinant nature of information causes plaintiffs' harms to elude courts. Such harms threaten the democratic relationship between citizen and state. However, the Court renewed its attention to data privacy in NASA v. Nelson*, in which the Court may have recognized a tension in its jurisprudence and rejected one of its precedents to better account for the harms and interests at stake.*

* Associate, Munger, Tolles and Olson LLP; J.D., Yale Law School, 2012; B.A., University of Michigan, 2009. The views expressed herein are solely those of the author and should not be attributed to the author's employer or its clients. The author thanks the Yale Law School Access to Knowledge Practicum for feedback throughout the stages of this article. She also thanks her family for their invaluable support.

15 YALE J.L. & TECH. 139 (2012) 2012-2013

TABLE OF CONTENTS

INTRODUCTION 141
I. A BARE AND CONFUSING DOCTRINE 143
A. The Supreme Court Pre-2011 143
1. Whalen v. Roe 143
2. Nixon v. General Services Administrator 146
B. The Supreme Court Speaks After Thirty Years in NASA v. Nelson 148
II. THE NATURE OF INFORMATIONAL PRIVACY 151
A. Data Traits Conceal Harm from Judicial Detection 153
B. Weakened Data Privacy Erodes Citizen-State Relations 154
III. ANY ROLE FOR *NASA?* 157
A. NASA *as Forming a Trilogy* 157
B. Resulting Flawed Balancing Test 158
1. The Individual's Interest 158
2. The Government's Interest 160
C. Displacing Nixon*:* NASA *as Forming a Sequel* 163
CONCLUSION 167

MOVING FROM *NIXON* TO *NASA*: PRIVACY'S SECOND STRAND—A RIGHT TO INFORMATIONAL PRIVACY

INTRODUCTION

Without her knowledge, a government clerk's blood is tested for HIV and pregnancy.[1] A police department asks an applicant about her off-duty sexual activities and for the name of the father of her miscarried child.[2] A public school posts a former employee's case of fibromyalgia on the internet and permits newspapers to broadcast the report.[3] Although data privacy[4] litigation and policy issues are increasing,[5] there is no consensus among the circuits as to the underlying privacy rights. They disagree broadly over which privacy interests are constitutionally protected, how to determine which interests are protected, and whether a right to informational privacy exists at all.[6] The Second, Third, Fifth, Seventh, and Ninth Circuits recognize a right to informational privacy and balance it against the state's interest;[7] the Sixth Circuit holds that the right only protects intrusions upon fundamental interests or those implicit in the concept of ordered liberty;[8] and the District of Columbia Circuit questions the existence of a constitutional right to privacy.[9]

Thirty years ago, the Supreme Court began to parse privacy interests and recognize an interest in nondisclosure of personal information in *Whalen v. Roe*, a case addressing a state's collection of citizen medical records.[10] This opinion was followed months later by another informational privacy case as the issue of whether the federal government could take custody of President Nixon's papers and screen the papers for archival purposes reached the Court in *Nixon v. General Services Administrator*.[11] After these two cases, the Court fell into a long silence on the issue. However,

---

[1] Norman-Bloodsaw v. Lawrence Berkeley Lab., 135 F.3d 1260 (9th Cir. 1998).
[2] Matson v. Bd. of Educ., 631 F.3d 57 (2d Cir. 2011).
[3] Coffman v. Indianapolis Fire Dept., 578 F.3d 559 (7th Cir. 2009).
[4] The right to nondisclosure, informational privacy, and data privacy are used interchangeably in the case law and literature. This Article will also use these terms interchangeably.
[5] ALEXEI PAVLICHEV & G. DAVID GARSON, DIGITAL GOVERNMENT: PRINCIPLES AND BEST PRACTICES 240 (2000) (explaining that as the government processes increasing amounts of public information, privacy issues continue to grow).
[6] For an overview of the "confusing and inconsistent" application of the right to informational privacy by circuit courts, see Gary R. Clouse, Comment, *The Constitutional Right To Withhold Information*, 77 NW. U. L. REV. 536 (1982).
[7] *See, e.g.*, Coffman v. Indianapolis Fire Dept., 578 F.3d 559, 566 (7th Cir. 2009); In Re Crawford, 194 F.3d 954, 959 (9th Cir. 1999); Barry v. New York, 712 F.2d 1554, 1559 (2d Cir. 1983); Fadjo v. Coon, 633 F.2d 1172, 1176 (5th Cir. 1981); and United States v. Westinghouse Electric Corp., 638 F.2d 570, 582 (3d Cir. 1980).
[8] *See, e.g.*, J.P. v. DeSanti, 653 F.2d 1080, 1090 (6th Cir. 1981).
[9] *See, e.g.*, Am. Fed'n of Gov't Emps. v. Dep't of Hous. & Urban Dev., 118 F.3d 786, 791 (D.C. Cir. 1997).
[10] Whalen v. Roe, 429 U.S. 589 (1977).
[11] 433 U.S. 425 (1977).

in 2011, the Supreme Court decided a third case on the right to informational privacy when it considered the constitutionality of the 9/11 Commission's recommended background checks of federal contractors in *NASA v. Nelson*.[12] In the intervening decades between *Nixon* and *NASA*, the circuits became increasingly divided in their data privacy jurisprudence. These divisions are not surprising given the scant guidance the Court provided in its initial foray into information privacy law. In both *Whalen* and *Nixon* the Court ruled in favor of the state, thereby avoiding setting a benchmark where protection for a right to nondisclosure might begin.

NASA presented an opportunity for the Court to confront foundational questions in information privacy law and democratic governance. However, the Court again assumed that a privacy right of constitutional significance was implicated and concluded that the government did not violate the right. These overarching similarities make it seem as though *NASA* merely replicates the Court's previous exiguous approach, bringing into question the legal impact of the case.

This Article examines the Supreme Court's information privacy jurisprudence, describing the complex characteristics of data and connecting these characteristics to the litigants' interests and the Court's difficulty in assessing those interests. The Article compares *Whalen*, *Nixon*, and *NASA* and finds that *NASA* is caught between conflicting precedents. Understanding *NASA* as responding to such a conflict leads to two principal interpretations of *NASA*'s legal impact. These competing interpretations create different accounts of privacy law, which in turn suggest strikingly different consequences for the future of privacy law. In one reading, *NASA* attempts to gloss over the tension in the case law and merge *Whalen* and *Nixon* into a balancing test approach to data privacy rights. This Article argues that the resulting balancing test is a) poorly adapted to the nature and prominence of the use of information, and b) creates a rigorous dichotomy between the parties in which it is almost impossible to vindicate an individual's privacy interest. Another, and more likely, reading of *NASA* confronts the tension in *NASA*'s precedents and adopts *Whalen*'s approach over *Nixon*'s. Under this interpretation, the *NASA* Court adopts and mimics a holistic, free-form approach from *Whalen* that more thoroughly accounts for the complexities of information and the elusive harms that flow from data privacy invasions. This approach focuses on whether disclosures involve public dissemination of the data as well as on the context and norms.

[12] 131 S. Ct. 746 (2011).

MOVING FROM *NIXON* TO *NASA*: PRIVACY'S SECOND STRAND—A RIGHT TO INFORMATIONAL PRIVACY

This Article proceeds in three Parts. Part I examines the case law on informational privacy. Part II discusses the nature of privacy, contending that the invisible, nonrivalrous and recombinant nature of information makes the effects of data privacy invasions difficult to perceive. Moreover, this Part suggests that data privacy rights have basic constitutional implications for the relationship between citizen and state, implications that are particularly acute as information collection and analysis become increasingly advanced and central to our system of governance.

Part III illustrates two ways of understanding *NASA*'s role in the Court's data privacy jurisprudence. It contends that while it is possible to read *NASA* as accepting both of its precedents, this reading is unlikely. Accepting *Nixon* entails adopting a balancing test, a test that is barely acknowledged in *NASA* and inevitably leads to casting the parties' interests at inappropriate levels of generality. Reading *NASA* as *Whalen*'s legitimate heir provides a holistic analysis informed by context and norms, considerations that help the Court consider complex data privacy interests in a fair and feasible way.

I. A BARE AND CONFUSING DOCTRINE

The Supreme Court has provided scant guidance on a right to informational privacy. As Justice Alito wrote, "[t]he Court announced the decision in *Nixon* in the waning days of October Term 1976. Since then, the Court has said little else on the subject of an 'individual interest in avoiding disclosure of personal matters.'"[13] Overall, the Court created a confusing, incomplete framework upon which the circuit courts have built an informational privacy doctrine that is inconsistent and untenable.[14]

A. The Supreme Court Pre-2011

1. Whalen v. Roe

In *Whalen*, the Court for the first time explicitly recognized an individual's interest in nondisclosure of information, one that is different from the familiar decisional privacy right exemplified by cases such as *Roe v. Wade*,[15] *Loving v. Virginia*,[16] *Griswold v.*

[13] *NASA*, 131 S. Ct. at 756.

[14] "State and lower federal courts have offered a number of different interpretations of *Whalen* and *Nixon* over the years." *Id.* at 756 n.9. *See also* Clouse, *supra* note 6, at 538 (detailing the circuit courts' "misapplication" of the right to informational privacy).

[15] 410 U.S. 113 (1973) (holding that a right to privacy under the Due Process Clause of the Fourteenth Amendment extended to a woman's decision to have an abortion).

Connecticut,[17] and *Pierce v. Society of Sisters*.[18] In *Whalen*, the New York State Legislature passed a law classifying potentially harmful drugs into five schedules.[19] Schedule I included highly abused drugs that serve no medical purpose and cannot be prescribed. The remaining schedules included drugs that have medicinal purposes but also have the potential for abuse. Under the Act, all prescriptions for Schedule II drugs needed to be made on a triplicate form with a copy for the prescribing physician, the pharmacy and the New York State Department of Health. Schedule II drugs included medicines used for migraine headaches, epilepsy, schizo-affective disorders, and narcolepsy. The amount of information included on the forms was extensively detailed and allowed for easy identification of a given patient. Information on the forms included a patient's name, address, and age; drug and dosage; prescribing physician; and dispensing pharmacy. When the Department of Health received the prescription forms, it logged the information and then recorded the data on tapes for processing by a computer. For five years the original forms were kept in a vault in a room with a locked wire fence and alarm system, after which the forms were to be destroyed. The tapes were stored in a locked cabinet and computers were kept offline when running the tapes. A statute and Department of Health regulation prohibited disclosure of the identity of the patients.

Plaintiffs, a group of patients prescribed Schedule II drugs, filed suit on the grounds that persons in need of medication would decline treatment out of fear for the misuse of computerized data and resulting stigmatization as drug addicts. The Southern District of New York enjoined enforcement of the Act as a violation of plaintiffs' constitutional privacy rights.[20] The U.S. Supreme Court unanimously reversed based on substantive due process and privacy concerns.[21] The Court chose to address the status of

[16] 388 U.S. 1, 12 (1967) (invalidating laws banning interracial marriages on the ground that to deny the fundamental freedom of marriage based on race "is surely to deprive all the State's citizens of liberty without due process of law").

[17] 381 U.S. 479 (1965) (invalidating a Connecticut law prohibiting the use of contraceptives on the ground that it violated the right to marital privacy).

[18] 268 U.S. 510, 510 (1925) (holding that a statute that requires every parent, guardian or other person having control of a child to send him to the public school in the district where he resides is an unreasonable interference with the liberty of the parents and guardians to direct the upbringing of the child and violates the Due Process Clause of the Fourteenth Amendment).

[19] New York State Controlled Substances Act of 1972, N.Y. PUB. HEALTH LAW § 3300 et. seq. (McKinney, Supp. 1976-77).

[20] Roe v. Ingraham, 403 F. Supp. 931 (S.D.N.Y. 1975) (reasoning that the relationship between patient and physician is accorded protection and the state's action was a needlessly broad sweep).

[21] The Court had jurisdiction under 28 U.S.C. §§ 1252, 2101(b) as there was a three-judge court in the district court.

privacy in the Constitution, noting that the constitutional right to privacy remains largely undefined[22] and then identifying types of constitutionally protected privacy interests. As the Court stated, "The cases sometimes characterized as protecting 'privacy' have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."[23] The Court considered neither interest to be implicated in this case.

In assessing the plaintiffs' interests in nondisclosure, the Court began by considering ways that the information could be disclosed publicly. In particular, the Court considered public disclosure of the data as a result of Health Department employees negligently or deliberately failing to maintain proper security.[24] In finding that these possibilities were not grounds for invalidating the statute, the Court reasoned that "there was no support in the record, or in the experiences of the two States [California and Illinois] that New York has emulated, for an assumption that the security provisions of the statute will be administered improperly."[25] This program was contrasted with a First Amendment case where public disclosure was *part* of the contested program;[26] here, public disclosure would result only from a violation of the statute. Accordingly, the Court distinguished between a case explicitly involving public dissemination and a case, such as the one before it, where the Court considered the *possibility* of unwarranted disclosure.

The Court next recognized that there was an outstanding issue: disclosing information to the employees of the New York Department of Health. The Court again made a distinction between disclosure to the public and disclosure to government officials. The Court allayed the concern regarding disclosure to the state by finding that this disclosure was not significantly different from prior law and that the disclosure is not "meaningfully distinguishable from a host of other unpleasant invasions of

[22] Whalen v. Roe, 429 U.S. 589, 599 n.24 (1977) (quoting Philip B. Kurland, *The Private I: Some Reflections on Privacy and the Constitution*, U. CHI. MAGAZINE, Autumn 1976 at 7, 8).
[23] *Id.* at 599.
[24] In addition, the Court considered use of the data as evidence in a judicial proceeding and disclosure as a result of the doctor, pharmacist or patient voluntarily revealing information. Neither one was considered grounds for invalidating the statute. The first was held to be a remote possibility that would not justify invalidating an entire identification program, and the second was not a change from prior law.
[25] *Whalen*, 429 U.S. at 601.
[26] *Id.* at 600 n. 27 (discussing *Buckley v. Valeo*, 424 U.S. 1 (1976)).

privacy that are associated with the many facets of health care."[27] While the Court's analysis concerning disclosure to the government was short, it considered context—which in this case was health care—and existing norms in determining that no right to informational privacy was violated.

The Court included a "final word" noting that it was aware of the threat to privacy that results from the vast accumulation of information by the government in computerized data banks or other government files.[28] It further stated that in some circumstances there is "arguably" a duty to avoid unwarranted disclosures.[29] The Court mentioned the collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws. In conclusion, the Court stated that it did not decide any question that would result from disclosure of private information or systems without comparable security provisions. Discussing such a significant concern in dicta is an indication that the Court is shying away from engaging with critical issues and providing substantive guidance to lower courts. Nonetheless, this concluding statement further hints at the significance of the distinction between disclosure to the government and to the public. In addition, addressing the vast accumulation of information in computer databanks evinces concern for bureaucratization, technology, and the power of information.

2. Nixon v. General Services Administrator

Only months after *Whalen*, the Court decided *Nixon*, a complicated case concerning separation of powers, presidential privilege, the First Amendment, Bills of Attainder, and privacy. After President Nixon resigned, President Ford signed into law the Presidential Recordings and Materials Act, which directed the General Services Administrator to take custody of President Nixon's papers and tape recordings. Under the Act, the Administrator was to process and screen the materials and, with the approval of Congress, determine public access to the materials. Since President Nixon's private materials were comingled with

[27] *Id.* at 602. The Court also rejected the argument that the patients' decisional interest was violated because the state had the power to completely prohibit Schedule II drugs, and in any event the state was not completely prohibiting this conduct. Furthermore, since many patients were still receiving prescriptions, the Court did not find that individuals were deterred from receiving medications under the Act.
[28] *Id.* at 605.
[29] *Id.*

more official materials,[30] any screening before President Nixon could sort and filter his papers and recordings would involve the screening of personal materials by the Administrator. Accordingly, although the Act required the Administrator to consider the need to protect constitutional rights, the Administrator and the archivist team would screen and analyze communications with the President's wife and clergyman as well as personal diary Dictabelts and the former first lady's personal files.

President Nixon claimed, among other things, that the Act violated his right to privacy under the First, Fourth and Fifth Amendments. The District Court of the District of Columbia found that the Act was facially constitutional,[31] but found the President's privacy claims to be the most troubling of all the issues.[32] In affirming the district court, the Supreme Court cited *Whalen* for the proposition that one element of privacy is avoiding disclosure of personal matters. The Court then cited *Katz v. United States*,[33] a Fourth Amendment search and seizure case, to determine that the President has a legitimate expectation of privacy. However, again citing Fourth Amendment case law,[34] the Court held that the invasion must be weighed against the public interest. It found that the privacy interest was weaker than in *Whalen* because not only was the information protected against undue dissemination, but also because the government would not retain long-term control over purely personal materials. The Court also believed the statute to be the least restrictive means for attaining the pertinent presidential material due to its comingling with private material.

The concurrence and dissent both accepted the majority's use of a balancing test, questioning only which public interests could outweigh President Nixon's privacy interests. The concurrence stated that mere historical significance is not sufficient for the government to retain personal materials, and that the majority was not holding as such because all personal information

[30] Prior to this statute, Presidents controlled which of their materials would be archived, therefore President Nixon had no reason to separate his personal and private communications.

[31] The court reasoned that the proportion of materials implicating privacy interests was quite small, as most of the materials related to Presidential duties to which "great public interest" attached. *Id.* at 358. Then, by explicitly performing a balancing test, the court found the intrusion reasonable because the public interest outweighed the President's privacy interests. The court also found that the measure was carefully tailored and was the least intrusive means to obtain the relevant information.

[32] Nixon v. Adm'r of Gen. Servs., 408 F. Supp. 321, 357 (D.D.C. 1976).

[33] 389 U.S. 347, 351-53 (1967).

[34] Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 458 (1977) (citing Terry v. Ohio, 392 U.S. 1 (1968); Camara v. Mun. Court, 387 U.S. 523 (1967), and Katz v. United States, 389 U.S. 347 (1967)).

was to be returned to President Nixon.[35] In his dissent, Chief Justice Burger described the public interest asserted by the government as a "generalized need" and believed the President's privacy interest outweighed this need.[36] Chief Justice Burger contrasted the case with *Whalen*, arguing that *Whalen* dealt with dangerous drugs rather than personal, private business and political confidences.[37] Thus, as the dissent indicates, *Nixon* is a difficult case because private information included in the screening was of no public import.

B. The Supreme Court Speaks After Thirty Years in NASA v. Nelson

The Court began *NASA* by harkening back to the privacy right cited in *Whalen* and *Nixon* and proceeded to find that the right was not violated in the case before it. In *NASA*, due to a new Department of Commerce Directive, employees working at the Jet Propulsion Laboratory (JPL) operated by the California Institute of Technology (CalTech) were subject to a standard federal background check. After 9/11, the government sought to increase security among its workforce by requiring contractors to undergo a National Agency Check with Inquiries (NACI), the same background check as federal civil servants. As JPL is owned by NASA and only operated by CalTech under a government contract, JPL contractors had to undergo the NACI. The contractors previously were not required to undergo such a background investigation.

The NACI involves a Standard Form 85 (SF-85) and an Investigative Request for Personal Information. The SF-85 requires information such as name, address, employment information, personal and professional references, citizenship and military service, and whether the employee has "used, possessed, supplied, or manufactured illegal drugs" in the last year, and, if so, details about the activity and "any treatment or counseling received."[38] The government then processes the information through FBI and government databases and sends questionnaires to former employers, schools, landlords, and references.

The Investigative Request for Personal Information, known as Form 42, is the questionnaire sent to former landlords and references and asks whether the recipient has "any reason to question" the employee's "honesty or trustworthiness," and

[35] *Nixon*, 433 U.S. at 484 (White, J., concurring).
[36] *Id.* at 529 (Burger, C.J., dissenting) (drawing language of "generalized need" from United States v. Nixon, 418 U.S. 683 (1974)).
[37] *Id.* at 533.
[38] NASA v. Nelson, 131 S. Ct. 746, 748 (2011).

whether the reference knows of any "adverse information" concerning the employee's violation of the law, financial integrity, abuse of alcohol and/or drugs, mental or emotional stability, general behavior or conduct, or other matters.[39] The form asks for an explanation regarding the presence of any of the above traits, as well as for derogatory or favorable information that may relate to suitability for government employment or security clearance. A "suitability matrix" was posted temporarily on the JPL intranet site that listed factors for suitability for federal employment. Factors included "carnal knowledge," "health issues," "mental, emotional, psychological, or psychiatric issues," and "criminal and immoral conduct." In addition, the document stated that "homosexuality," "adultery," and "illegitimate children" might pose security issues if there could be "susceptibility to coercion or blackmail."[40] Although the suitability matrix was removed from the JPL site and the issue was not considered before the Court, the Court mentioned the matrix in its opinion[41] and the issue was extensively briefed. Indeed, the broad factors listed on the suitability matrix and open-ended inquiries on Form 42 demonstrate the expansiveness of the government's data collection. The suitability matrix also demonstrates how easily information is susceptible to unforeseen and questionable uses as the data can be used and manipulated almost without limit.[42]

On the other hand, information on the SF-85 and Form 42 is provided some protections. The information is governed by the Privacy Act, which permits the government to keep records which are "relevant and necessary" to an end "required by law" and permits disclosure of an individual's records without consent only in certain instances. Under the Act, individuals can access their records and request amendments.[43]

The plaintiffs claimed that this background check violated their right to informational privacy, but the Supreme Court disagreed, reversing the Ninth Circuit's preliminary injunction of

---

[39] *Id.* at 749.
[40] *Id.* at 754 n.5.
[41] *Id.*
[42] This is due to the recombinant and nonrivalrous nature of data, *see infra* Section II.
[43] Notably, a common complaint is that the Privacy Act has inadequate coverage and enforcement. One example is that agency officials have broadly interpreted the routine use clause for agency sharing such that they have "created almost unlimited ability to move data among Federal agencies." HAROLD C. RELYEA, CONG. RESEARCH SERV., RL30824, THE PRIVACY ACT: EMERGING ISSUES AND RELATED LEGISLATION 9 (2002). *See also* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1167 (2002) (noting drawbacks of the Privacy Act, such as its inapplicability to court records and to information that FOIA requires to be released).

the background checks. The Court focused on two factors—that the government was acting in its capacity as an employer and that the information is subject to the Privacy Act's nondisclosure requirement. The Court emphasized that the government has a "freer hand" when acting as proprietor and manager of its internal operations than when it "brings its sovereign power to bear on citizens at large."[44] It further held that the distinction between employee and contractor is a formalism that has no effect here; rather, what is important is that the Court finds that the JPL employees perform work "critical to the NASA mission."[45] The Court considered the SF-85 inquiry into drug treatment to be a reasonable, employment-related inquiry since it works to identify which employees are taking steps to overcome a drug problem, and *Whalen* held that measures need not be necessary or the least restrictive means of furthering the government's interests.[46] The Court then found the open-ended questions to be a reasonable measure for differentiating between strong and weak candidates, reasoning that a catalog of questions is daunting and that the prevalence of similar forms in the private sector evinces the propriety of the forms.

After determining the reasonableness of the government's inquiries "in light of the . . . interests at stake,"[47] the Court stressed the Privacy Act's protections against disclosure to the public. The Court found that *Whalen* and *Nixon* indicate that statutory duties "generally allay" privacy concerns.[48] Furthermore, the many statutory exceptions to the Privacy Act's nondisclosure bar are not significant because an "ironclad disclosure bar" is not required and the plaintiffs did not put forth a "plausible scenario" where there would be undue disclosures.[49] Similar to the Court in *Whalen*, the Justices did not vigorously scrutinize the protections of the Act, but rather seemed to adopt a presumption of its adequacy. The Justices also did not take into account increasing technology or bureaucratization of the state, concerns expressed in the "final word" of the *Whalen* opinion, to consider how the likelihood of undue disclosures might change.

In his concurrence, Justice Scalia argued that there is no right to informational privacy;[50] he considered the collection of

[44] *NASA*, 131 S. Ct. at 757-58 (quoting Engquist v. Oregon Dept. of Agric., 553 U.S. 591, 598 (2008)).
[45] *Id.* at 750.
[46] *Id.*
[47] *Id.* at 761.
[48] *Id.*
[49] *Id.* at 763.
[50] *Id.* at 765 (Scalia, J., concurring). Justice Scalia reasoned that the Due Process Clause only protects procedural rights and that "mere disclosure of private information" would not invoke procedural protections since defamation does not qualify for such protections. Justice Thomas also argues that the Constitution

information here to be a problem under the Fourth Amendment.[51] This distinction between a Fourth and Fifth Amendment challenge contrasts with the reasoning in *Nixon,* which blended the two Amendments together. It also illustrates the general confusion as to where privacy interests lie.

II. THE NATURE OF INFORMATIONAL PRIVACY

Important in the adjudication of privacy interests is the consideration of the meaning and purpose of privacy and, more precisely, data privacy. Louis Brandeis and Samuel Warren first recognized a right to privacy in their famous 1890 *Harvard Law Review* article, describing privacy as the "right to be let alone."[52] Cogent as this definition may be, it provides little legal guidance.[53] Indeed, the concept of privacy has been a particular quagmire for the development of legal doctrine, which has been described as exploring an unknown swamp[54] and as indefinable.[55] How amenable privacy is to definition remains an open question, but the prolonged irresolution to date evinces its elusive and multi-faceted nature. Robert Post relays that "[p]rivacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings" that he "despair[s] whether it can be usefully addressed at all."[56] Indeed, privacy interests pervade the Constitution from its penumbras[57] to the First,[58]

---

does not protect a right to informational privacy. *Id.* at 769 (Thomas, J., concurring).

[51] Yet even under the Fourth Amendment Justice Scalia did not recognize a constitutional violation because he found that inquiring with third parties as part of the background investigation does not fall within the meaning of Fourth Amendment searches. *Id.* at 765 (Scalia, J., concurring).

[52] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

[53] ELLEN ALDERMAN & CAROLINE KENNEDY, THE RIGHT TO PRIVACY, at ii (1997).

[54] JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 3 (1992).

[55] SERGE GUTWIRTH, PRIVACY AND THE INFORMATION AGE 41 (2002).

[56] Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2087 (2001).

[57] *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965) (invalidating a Connecticut law that prohibited the use of contraceptives on the ground that it violated the right to marital privacy found in the "penumbras" and "emanations" of other constitutional protections).

[58] U.S. CONST. amend. I ("Congress shall make no law . . .abridging the freedom of speech . . . or the right of the people peaceably to assemble . . . ."); *see, e.g.*, NAACP v. Alabama, 357 U.S. 449 (1958) (holding that the state could not force the NAACP to disclose membership lists as the individuals have a right to privacy that protects them from harassment).

Third,[59] Fourth,[60] Fifth,[61] Ninth,[62] and Fourteenth[63] Amendments. Unsurprisingly, the judiciary has struggled to adjudicate privacy interests. In an effort to clarify the law, the Supreme Court recognized in *Whalen* "at least two" kinds of privacy interests rooted in the Due Process Clause: "[O]ne is the individual interest in avoiding disclosure of personal matters, the other is the interest in independence in making certain kinds of important decisions."[64] Thus, the Court formulated a rudimentary definition of an informational privacy interest as avoiding disclosure of personal matters and located the interest within the Fifth and Fourteenth Amendments.

---

[59] U.S. CONST. amend. III ("No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.").

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

[61] U.S. CONST. amend. V ("No person shall be … compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law . . . ."). For an example of the Court upholding one's right not to testify against oneself, see *Miranda v. Arizona*, 384 U.S. 436, 444 (1966), stating that "[U]nless other fully effective means are devised to inform accused persons of their right of silence and to assure a continuous opportunity to exercise it . . . . Prior to any questioning, the person must be warned that he has a right to remain silent, that any statement he does make may be used as evidence against him, and that he has a right to the presence of an attorney, either retained or appointed.". For examples of data privacy under the Fifth Amendment, see *Nixon v. Administrator of General Servs*., 433 U.S. 425 (1997), applying *Whalen*'s recognition of an interest in nondisclosure of personal information rooted in the due process clause of the Fifth Amendment.

[62] U.S. CONST. amend. IX ("The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."); *see, e.g.*, Griswold v. Connecticut 381 U.S. 479, 491 (1965) (Goldberg, J., concurring) ("To hold that a right so basic and fundamental and so deep-rooted in our society as the right of privacy in marriage may be infringed because that right is not guaranteed in so many words by the first eight amendments to the Constitution is to ignore the Ninth Amendment and to give it no effect whatsoever.").

[63] U.S. CONST. amend. XIV § 1 ("[N]or shall any State deprive any person of life, liberty, or property, without due process of law . . . ."); s*ee, e.g.*, Lawrence v. Texas, 539 U.S. 558 (2003) (sexual acts committed in the privacy of the home cannot be criminalized because it violates the Fourteenth Amendment's liberty and privacy rights); Whalen v. Roe, 429 U.S. 589 (1977) (recognizing an interest in nondisclosure of personal information rooted in the due process clause); Roe v. Wade, 410 U.S. 113 (1973) (holding that a liberty interest protects a woman's right of privacy to have an abortion in her first trimester of pregnancy).

[64] *Whalen*, 429 U.S. at 599.

A. Data Traits Conceal Harm from Judicial Detection

While the *Whalen* Court helped provide a legal structure for unpacking privacy interests via classifying such interests into particular genera, the complex nature of privacy, as well as of information, still troubles courts. The complexity of informational privacy is inherent in the nature of information itself: it is nonrivalrous, invisible and recombinant. These traits effectively blind judges to the harms at stake in data privacy cases.

Firstly, information is a nonrival good in that there can be simultaneous users of the good; that is, one person's use of a piece of information does not make it less available to another.[65] Moreover, data privacy invasions are difficult to detect because they can be invisible. Information can be accessed, stored, and disseminated without notice.[66] The ability of information to travel at the speed of light enhances the invisibility of data access--that is, information collection can be the swiftest theft of all. Consequently, together, the invisible and nonrivalrous consumption of information allows for massive privacy invasions without any obvious harm to the invaded individuals.

Furthermore, information is recombinant: that is, data output can be used as an input to generate more data output, and so forth.[67] For instance, through a developing application known as Knowledge Discovery and Data Mining processes, data can be combined to "create facts" about an individual; in particular, the

---

[65] For a description of how information is a nonrival good, see YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 36 (2006). However, in the strict economic sense, spreading information could potentially diminish the value of that information in certain circumstances, such as in the case of groundbreaking news or a scientific discovery. *See, e.g.*, Int'l News Serv. v. Associated Press, 248 U.S. 215, 239-40 (1918) (holding that when a news service republishes information attained from another new service it is "endeavoring to reap where it has not sown" at the expense of "those who have sown"); Barclays Capital Inc. v. Theflyonthewall.com, 700 F. Supp. 2d 310 (S.D.N.Y. 2010), *rev'd*, 650 F.3d 876 (2d Cir. 2011) (applying the hot news misappropriation doctrine to a financial news aggregation website using data produced from other financial firms). The relevant point here is that users can possess information without limiting any other user's actual possession of that piece of information.

[66] *See* Solove, *supra* note 43, at 1194 (explaining that sometimes an individual is not even aware that an institution maintains a record about her as she often may not see it).

[67] WILLIAM LANDES & RICHARD A. POSNER, THE POLITICAL ECONOMY OF INTELLECTUAL PROPERTY LAW 15 (2004) (noting that creators of intellectual property use the intellectual property of others as inputs into their creation); *see also* MARTIN KUHN, FEDERAL DATAVEILLANCE: IMPLICATIONS FOR CONSTITUTIONAL PRIVACY PROTECTIONS 172 (2007) (explaining how a terrorist's information is retrieved and used in conjunction with other terrorists' information to form a pattern, which is then used to assign probabilities to predictors in order to build a profile for possible terrorists).

likelihood that an individual will engage in a certain type of behavior.[68] The creation of new knowledge complicates data privacy law as it involves information the individual did not possess and could not disclose, knowingly or otherwise. In addition, as our state becomes an "information state" through increasing reliance on information—such that information is described as the "lifeblood that sustains political, social, and business decisions"[69]—it becomes impossible to conceptualize all of the possible uses of information and resulting harms.[70] Such a situation poses a challenge for courts whom are effectively asked to anticipate and remedy invisible, evolving harms.

B. Weakened Data Privacy Erodes Citizen-State Relations

Asking courts to remedy the invisible, evolving harms of data privacy invasions requires examining what the types of harms *are*. If the harms are difficult to perceive, it is tempting to see them as insubstantial. However, such an assumption ignores the effect informational privacy interests have on the relationship between citizen and state,[71] especially the balance of power between the two. Almost forty years ago one court recognized that "the increasing complexity of our society and technological advances . . . facilitate massive accumulation and ready regurgitation of far-flung data," presenting problems "not anticipated by the framers of

[68] KUHN, *supra* note 67, at 173.

[69] Elbert Lin, Note, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1091 (2002) (quoting FRED H. CATE, PRIVACY IN THE INFORMATION AGE 5 (1997)).

[70] Among other things, information can be used to hack credit card accounts or for identity theft generally. For example, on October 25, 2012 the South Carolina Department of Revenue Agency announced that its database was hacked and about 3.6 million Social Security numbers and some 387,000 credit and debit card numbers of taxpayers were obtained. Andrew M. Ballard, *About 3.6 Million SSNs Exposed in Hack Of South Carolina Tax Agency's System,* BLOOMBERG BNA, Nov. 5, 2012, http://www.bna.com/36-million-ssns-n17179870754/. The cyber-attack prompted the Governor to issue an executive order upbraiding the state's information technology policy, expressing that the "state government's fragmented approach to IT security makes South Carolina vulnerable to serious cyber and information breaches and requires immediate action to minimize cyber-attacks on IT infrastructure and records." State of South Carolina, Exec. Order No. 2012-10, http://governor.sc.gov/ExecutiveOffice/Documents/2012-10%20Reviewing%20IT%20Security.pdf.

[71] While corporate practices also pose concerns regarding an individual's privacy, the relationship between individual and government is of constitutional import. Adjudicating privacy rights against corporate actors is another avenue for research.

the Constitution."[72] The court further noted that "[t]hese developments emphasize a pressing need to preserve and redefine aspects of the right of privacy to insure the basic freedoms guaranteed by this democracy."[73]

The connection between informational privacy and democratic freedoms stems from the prominent role data plays in governance and power. Harlan Cleveland argues that:

> Government *is* information. Its employees are nearly all information workers, its raw material is information inputs, its product is those inputs transformed into policies, which are simply an authoritative form of information. So in a narrow sense, to consider government information policy is not far from considering the essence of government itself.[74]

Moreover, the combination of technology with control of data flow has been described as a "tool of enslavement" for society if the power is abused.[75] This dynamic can be observed in the classic case of a bribe—if *X* is aware of a potentially embarrassing or personal fact, or even myth, regarding *Y*, *X* can bribe *Y* in exchange for not using or disseminating the information pertaining to *Y*. The released Guantanamo prisoners who struggled for a

---

[72] Menard v. Mitchell, 328 F. Supp. 718, 725 (D.D.C. 1971) (footnotes omitted), *rev'd on other ground sub. nom.* Menard v. Saxbe, 498 F.2d 1017 (D.C. Cir. 1974).

[73] *Id.* A few years later the executive Privacy Protection Study Commission echoed this sentiment, "[N]ew avenues and needs for collecting information, particularly when coupled with modern information technology, multiply the dangers of official abuse against which the Constitution seeks to protect. . . . [W]hile our efforts to protect ourselves against them must ultimately be fashioned into law, the choices they require are not mere legal choices; they are social and political value choices of the most basic kind." PERSONAL PRIVACY IN AN INFORMATION SOCIETY: THE REPORT OF THE PRIVACY PROTECTION STUDY COMMISSION (1977), *available at* http://aspe.hhs.gov/datacncl/1977privacy/c1.htm.

[74] Harlan Cleveland, *Government is Information (But Not Vice Versa)*, 46 PUB. ADMIN. REV. 605, 605 (1986); *see also* Lillian R. BeVier, *Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection*, 4 WM. & MARY BILL RTS. J. 455 (1995) ("Information supplied by citizens to government is the indispensable handmaiden of the modern activist state.").

[75] Robert S. Peck, *Extending the Constitutional Right to Privacy in the New Technological Age*, 12 HOFSTRA L. REV. 893, 987 (1983-84). A well-known literary example is the Orwellian surveillance state, which epitomizes how the lack of privacy transforms how a community functions. In *1984*, the state holds access to practically unlimited information about each person, enabling the state to identify and track anyone with even a scintilla of suspected disloyalty to the government. Furthermore, Orwell sharply captures how information control makes the past mutable as the government changes historical facts about individuals and events. GEORGE ORWELL, 1984 (1949).

country to allow them into their borders illustrates a more extreme case.[76] The released prisoners' rejection reveals how merely associating an individual with a possible set of facts, even untrue facts, can significantly impact an individual's liberty and future societal integration. Thus, data access can easily empower the receiver while dangerously degrading the individual to whom the data pertains.

Moreover, the reliance on data to understand individuals impacts our concept of personhood. Information and data flow are increasingly central to social and economic ordering as individuals become identified by an extensive set of information such as tax records, voting eligibility, and government-provided entitlements.[77] One scholar argues that the ways in which our digital biographies are used results in growing dehumanization, powerlessness, and vulnerability for individuals.[78] This phenomenon points to an emerging link between data collection and the construction of personhood. Unfortunately, the effect on personhood is reducing individuals to mere composites of transactional data, debasing our understanding of individual and citizenship. Such debasement also carries with it the risk of misrepresentation. Information is liable to distortion and can be taken out of context. For example, quick impressions and fragments of information are likely to "oversimplify and misrepresent our complicated and often contradictory characters."[79] In effect, data collection and analysis can be a demoralizing process and can create a false image of an individual. Thus, broad government access to an individual's information can significantly upset the delicate balance of power in a democracy between citizen and state.

Informational privacy is a complex concept that is prone to elusive harms. The judiciary has struggled for over three decades to create a viable legal construct to define and consider such harms. The lack of a viable construct is troubling given the

[76] Lara Setrakian, *Guantanamo's Innocents: Newly Released Prisoners Struggle to Find a Home*, ABC NEWS, May 23, 2006, http://abcnews.go.com/International/story?id=1997083.

[77] Solove, *supra* note 43, at 1143-47; *see also* Charles A. Reich, *The New Property*, 73 YALE L.J. 733, 733-37 (1964) (discussing the increase in government entitlements and licensing).

[78] Solove, *supra* note 43, at 1141.

[79] JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 9 (2000). Harlan Cleveland describes information as compressible in that information can be concentrated, integrated, summarized, and miniaturized. The risk of such compression is that "[I]nformation is bound to be lost [and] what is lost may turn out to be trivial or merely interesting, but it could also turn out to be critically relevant." Harlan Cleveland, *Information as a Resource*, THE FUTURIST, Dec. 1982, at 34, 37.

advanced data collection systems that continue to emerge. If the judiciary is going to play a role in understanding data privacy interests and balancing power between citizen and government, it is time to assess its doctrine.

III. ANY ROLE FOR *NASA?*

Over the thirty years between *Nixon* and *NASA* a wealth of data privacy cases surfaced in the lower courts. However, the Court did not resolve the split among the circuits in its *NASA* decision last year. The lower courts have spoken back, one asserting that "the verdict on informational privacy [after *NASA*] is an unequivocal 'who knows' . . . . and leaves unresolved a circuit split containing a wide range of opinions,"[80] and another asserting that *NASA* "has not provided [this circuit] with any reason to . . . revisit our past precedents . . . ."[81] Thus, the question arises as to what, if anything, *NASA* contributes to data privacy jurisprudence.

The answer may be what the above courts proclaim: *NASA* offers very little, merely continuing the Court's haphazard approach. On the other hand, one may see the Court as identifying and responding to tension between *NASA*'s precedents. Upon close examination it appears that *Whalen* and *Nixon* fundamentally conflict, and that this conflict lies at the heart of the circuit split. That is, *Nixon* clearly invokes a balancing test and Fourth Amendment case law to protect privacy interests, while the approach taken in *Whalen* does not explicitly invoke either of these, engaging instead in a broader, more fluid analysis. In this vein, one could view *NASA* as a tiebreaker case that entrenches certain principles in informational privacy jurisprudence. However, which principles *NASA* adopts is unclear. This Article argues that there are two principal interpretations of *NASA*. One interpretation is that the *NASA* Court is attempting to piece together a balancing test from both *Whalen* and *Nixon* to solidify a uniform approach. In another interpretation, the Court is adopting *Whalen* over *Nixon*, eschewing a Fourth Amendment analysis. These contrasting approaches provide different possibilities for the Court's ability to work through data privacy issues.

A. NASA *as Forming a Trilogy*

One interpretation of *NASA* is that it weaves *Whalen* and *Nixon* together to form a balancing test for constitutional information privacy claims. Already *NASA* has been described as employing a type of balancing test by Justice Scalia, as his concurring opinion in *NASA* characterized the Court's approach as

[80] Elkins v. Elenz, No. 8:11 Civ. 2817 (M.D. Fla. July 19, 2012).
[81] Lee v. City of Columbus, 636 F.3d 245, 260 n.8 (6th Cir. 2011).

invoking a "never-explained assumption that the Constitution requires courts to 'balance' the Government's interests in data collection against its contractor employees' interest in privacy."[82] Although it is not clear that *NASA* adopts such an approach, it is possible to understand the Court's analysis in this way. However, this interpretation has severe limitations in its understanding of the parties' interests, as it casts the individual's interest at an inappropriately low level of generality while casting the government's interest at inappropriately high level of generality.

NASA can be understood as performing a balancing test since the Court rules in favor of the government after finding the government's interest to be "strong"[83] and the contractors' privacy concerns to be "allay[ed]."[84] In the Court's view, the fact that the government was acting as proprietor and the contractors performed "critical" roles at *NASA*, such as serving as the lead trouble-shooter for the $568 million Kepler Space Observatory, gave the government a strong interest in the conduct of the contractors. Also, the Court noted that the investigation was instituted in response to a recommendation by the 9/11 Commission,[85] and considering that the Government's brief emphasized security concerns,[86] it can be surmised that security factored into the government's interest as well. In addition, the Court cited *Whalen* to support its reasoning that the protections of the Privacy Act, namely the nondisclosure obligations, "evidence a proper concern for privacy interests"[87] and thereby generally allay privacy concerns. Overall, these evaluations of the strength of the parties' interests, in conjunction with a determination that the inquiries are reasonable, could be understood as a balancing test.

B. Resulting Flawed Balancing Test

1. The Individual's Interest

A closer look at the Court's conceptualization of the individual's interest in *NASA*, *Nixon,* and *Whalen* for purposes of a balancing test reveals that not only are there strong doubts as to

[82] NASA v. Nelson, 131 S. Ct. 746, 764 (2011) (Scalia, J., concurring). Several circuits attempted to read *Whalen* and *Nixon* as putting forth a balancing test even before *NASA*. See sources cited *supra* note 7.
[83] *NASA*, 131 S. Ct. at 759 (majority opinion).
[84] *Id.* at 761.
[85] *Id.* at 752.
[86] The reply brief notes that "the terrorist attacks of September 11, 2001[] revealed security vulnerabilities in federal facilities . . . ." Reply Brief for Petitioners at 10, NASA v. Nelson, 131 S. Ct. 746 (2011) (No. 09-530).
[87] *NASA*, 131 S. Ct. at 762.

whether *NASA* integrates both of its predecessors,[88] but also that such an interpretation has dangerous consequences. Interpreting *NASA* as performing a balancing test requires conceiving of the parties' interests in a starkly bifurcated manner of citizen versus state that distorts the interests at stake and closes off a consideration of the complex nature of data traits.

When the Court considers the individual's interest in the data privacy cases, it is always based on the individual's concern for the data in the abstract. Such an approach debases the individual's interest because it fails to take into account data aggregation. Yet, due to the recombinant nature of information, collected pieces of data can be continuously combined with one another, as well as with other information available to the government, to reveal further information about individuals. Daniel Solove explains how privacy can be endangered by combining "relatively innocuous bits of information" as the combination paints "a rather detailed portrait of our personalities and behavior." [89] Solove calls this problem "aggregation" and notes that businesses and government often aggregate a variety of information fragments, including pieces of information we would not view as private in isolation, to paint such a portrait.[90] This is especially relevant as the U.S. is an advanced information state,[91] such that fragments of information are readily available and easy to combine.[92] The Court itself can be seen struggling with a concern for privacy in the context of an increasingly bureaucratic and technological state. Thirty years ago the Court was troubled with the problem that vast data keeping and computerized files posed for privacy, writing, "[w]e are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files," and citing sources describing the assault on privacy.[93]

---

[88] *See infra* Section III.B.

[89] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 70 (2008).

[90] *Id.*

[91] *See* Solove, *supra* note 43, at 1143 (2002) ("[T]he expansion of the bureaucratic network of regulation, licensing, and entitlements at the federal, state, and local levels resulted in a massive escalation of public records . . . .").

[92] *See* Transcript of Oral Argument at 45, IMS v. Sorrell, 131 S. Ct. 2653 (2011) (No. 10-779) (Sotomayor, J.) ("Today with the Internet and with computers, there's virtually no privacy individuals have. Any transaction you do could be spread across the world instantaneously."). The ability to manipulate information via data mining raises a new level of concerns for individuals and courts beyond the revelation of a single fact; rather, behavioral probabilities can be assigned to individuals. KUHN, *supra* note 67, at 173. For an example of a case grappling with data mining and pattern matching processes see IMS v. Sorrell, 131 S. Ct. 2653 (2011), a First Amendment privacy case.

[93] Whalen v. Roe, 429 U.S. 589, 605 & n.34 (1977) (citing Barry B. Boyer, *Computerized Medical Records and the Right to Privacy*: *The Emerging Federal*

The Court also casts the individual's interest at too low a level of generality because it fails to take into account the full consequences of disclosure to the government. The Court merely considers the individual's reputational concerns.[94] *Whalen*, the seminal case on an informational privacy right, considered whether the reputational impact of the statutory patient-identification program on Schedule II drug patients was sufficient to be an invasion of any right protected by the Fourteenth Amendment.[95] But, as discussed above, privacy runs much deeper than reputation; it is integral to maintaining the appropriate balance of control in citizen-state relations even when there is no disclosure of information to the public.[96] For instance, unmasking bits of an individual's identity creates an informational advantage in the state that threatens basic democratic liberties.[97] Moreover, becoming associated with bits of data degrades an individual's personhood, while the holder of the data has the ability to manipulate the information in Orwellian, self-serving ways. In effect, the Court overlooks critical concerns; the Court analyzes the individual's interest in data privacy in a shallow fashion and marginalizes the deeper interest in preventing *any* disclosure of information.

2. The Government's Interest

In contrast to the Court's narrow description of the individual's interest in data privacy cases, the Court casts the government's interest at too high a level of generality and also fails to aptly scrutinize the interest. Correctly classifying the government's interest without being lured into broad, lofty descriptions such as "national security" or "war on drugs" may be difficult whenever the government litigates on behalf of the public interest. *NASA* is an illustrative case study as it grapples with the government's asserted interest in security, one of the most prominent justifications today for invasions of privacy.[98] In *NASA*,

---

Response, 25 BUFF. L. REV. 37 (1972); Arthur R. Miller, *Computers, Data Banks and Individual Privacy: An Overview*, 4 COLUM. HUM. RTS. L. REV. 1 (1972); and ARTHUR R. MILLER, THE ASSAULT ON PRIVACY (1971)).

[94] The Court's limited consideration may be partly attributable to the parties' failure to raise broader issues in their briefs.

[95] *Whalen*, 429 U.S. at 603-04. *Whalen* considers an interest in independence, but this consideration is not in regards to informational privacy, but for decisional privacy.

[96] *See supra* Section II.B.

[97] *Id.* Alex Aleinikoff describes the Court's attempt to quantify immeasurable litigant interests (such as privacy and other civil rights) and "strike the unstrikeable balance" in its balancing test as depreciating the value of some of the interests at stake. Alex Aleinikoff, *Constitutional Law in the Age of Balancing*, 96 YALE L.J. 943, 975 (1987).

[98] Another example is the U.S. Department of Homeland Security Secure Flight Program, which requires all airlines to provide a passenger's name, date of birth,

the federal government made its background investigations applicable to contractors in response to a recommendation by the 9/11 Commission,[99] and in response the Court found that the government has an interest in "securing its facilities."[100] Thus, *NASA* is one manifestation of the outburst of concern for terrorism post-9/11 that provided a platform for the government to accumulate broad powers to surveil individuals and collect data.[101] Indeed, the threat anonymity can pose for national security indicates why the government sought to "know" each of its employees and contractors.[102] Accordingly, national security has become a formidable interest with which to contend, whereby even concerns regarding torture struggle to compete with security justifications.[103] However, the formidable nature of a national security interest should cause courts to invoke it cautiously, especially with respect to informational privacy claims where the

---

gender, and known redress number to the Transportation Security Administration. *Secure Flight Program*, U.S. DEP'T OF HOMELAND SECURITY, http://www.dhs.gov/files/programs/gc_1250693582433.shtm (last visited Jan. 3, 2013).

[99] NASA v. Nelson, 131 S. Ct. 746, 752 (2011).

[100] *Id.* at 758 (citing Engquist v. Oregon Dept. of Agric., 553 U.S. 591, 598-99 (2008)).

[101] The passage of the USA Patriot Act, release of the 9/11 Report, and passage of the Intelligence Reform and Terrorism Act of 2004 caused an increase in government-mandated information sharing among branches, agencies and departments within the government to improve intelligence and law enforcement. *See generally* RICHARD A. BEST JR., CONG. RESEARCH SERV., R41295, INTELLIGENCE REFORM AFTER FIVE YEARS: THE ROLE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (2010).

[102] *See, e.g.*, DENNIS BAILEY, THE OPEN SOCIETY PARADOX 26-27 (2004) ("[A]nonymity has become one of the central vulnerabilities of an open society. Freedom may have allowed [the 9/11 terrorists] to rent an apartment, use a cell phone, meet with terrorists overseas . . . but anonymity kept hidden the manner in which these individuals' actions fit together into a larger mosaic of death.").

[103] There is an active debate regarding justifying the use of torture in the War on Terror. Alan Dershowitz, a civil libertarian, argues in favor of torture under controlled circumstances because there is little possibility that potentially catastrophic attacks can be deterred by "the threat of retaliation against a phantom enemy who welcomes martyrdom" and that a democratic nation surely should not simply wait until an "armed attack occurs" and then engage in retaliatory self-defense. Alan Dershowitz, *Should We Fight Terror with Torture?*, THE INDEPENDENT, July 3, 2006, http://www.independent.co.uk/news/world/americas/alan-dershowitz-should-we-fight-terror-with-torture-406412.html. In contrast, the President of the Supreme Court of Israel, Aharon Barak, in holding that torture could not be justified even for securing information to prevent terrorism, stated that "[A]lthough a democracy must often fight with one hand tied behind its back, it nonetheless has the upper hand. Preserving the Rule of Law and recognition of an individual's liberty constitutes an important component in its understanding of security. At the end of the day, they strengthen its spirit and its strength and allow it to overcome its difficulties." HCJ 5100/94 Public Comm. Against Torture v. State of Israel 53(4) PD 817, 845 [1999] (Isr.).

harms to the individual are not easily recognizable. To its credit, the *NASA* Court did not accept the government's invitation to dwell at length on 9/11 concerns,[104] and the Court emphasized the government's role as an employer. Yet despite the Court's emphasis on the employment context, allowing even a backdrop of security concerns in *NASA* makes for a remarkable characterization of the government's interest given that the NASA facility is operated by a university and engages in scientific research such as "the star formation of the history of the universe."[105] Such facts should make the government's interest in *NASA* follow more along the lines of an interest in a competent workforce and less like a security matter of concern to the 9/11 Commission.

Moreover, asserting a national security interest can have dubious applications as the data collection may actually *diminish* the nation's and the plaintiffs' security. The risk of leaked information and lost civil liberties[106] are familiar problems with government data collection practices. The recent disclosures via WikiLeaks illustrate how the government's collection of massive amounts of data in one place or network presents a significant vulnerability if that location or network is comprised. Just last year WikiLeaks released on its website, among other things, a trove of confidential U.S. documents. From the WikiLeaks website "sprang everything from Iraq War logs, to profiles of Guantánamo Bay prisoners, to the infamous cables sent from the American Embassy in Tunisia confirming widespread government corruption . . . ."[107] The WikiLeaks situation demonstrates that the vulnerability of

[104] See sources cited *supra* note 86 and accompanying text.

[105] *NASA*, 131 S. Ct. at 752.

[106] Mention of another parallel to the torture debate is apt here. Some commentators argue that torture enhances security while others argue that torture diminishes security. Senator John Kerry argues that "Torture plays directly into a central tenet of al Qaeda's recruiting pitch: that everyday Muslims across the world have something to fear from the United States of America." John Kerry, *Commentary: Torture Weakened America's National Security*, CNN (Jan. 25, 2009), http://articles.cnn.com/2009-01-25/politics/kerry.guantanamo_1_abu-ghraib-torture-guantanamo-bay-prison?s=PM:POLITICS. In contrast, Alan Dershowitz argues that torture may be necessary to combat evolving threats and that human-rights organizations often fail to distinguish between "civilian deaths accidentally caused by democracies despite their best efforts to avoid them, and civilian deaths deliberately caused by terrorists who seek to maximise civilian casualties by constructing anti-personnel bombs, designed to kill as many innocent people as possible, and by specifically targeting crowded buses and other soft targets." Dershowitz, *supra* note 103.

[107] Jared Keller, *Is the Era of Government Secrets Over?*, THE ATLANTIC, (June 20, 2011, 8:40 AM), http://www.theatlantic.com/politics/archive/2011/06/is-the-era-of-government-secrets-over/240674/; *see also* Cleveland, *supra* note 79, at 37 (describing information as "diffusive" as it "tends to leak" and "striv[es] to break out of the unnatural bonds of secrecy").

government data at this level of magnitude is not just a possibility, but real in the here and now.

A general problem with balancing is that it involves the Court in a policy discussion, where it assesses the value of the government's interest.[108] Thus, the Court finds itself in a predicament when it invokes a balancing test: it must either engage in a policy analysis or rubber-stamp the government's asserted interest. Hence, we find the Court accepting the government's assertion of broad, lofty interests.

In summary, if the Court is applying a balancing test, the attendant conceptualization of the parties' interests is flawed. The individual's privacy interest is cast at too low a level of generality and the ultimate consequences of disclosure for the individual are glossed over. In contrast, the government's interest is cast at too high a level of generality and not adequately scrutinized. If the Court determines that it will proceed with a balancing test, the above analysis at least illustrates how its application in this context requires vetting.

A strong case can be made, however, that a balancing test is fundamentally incompatible with the notion of data privacy rights.[109] A balancing test requires a bifurcated analysis, where two separate interests are starkly distilled and opposed. This is detrimental in informational privacy cases because the harms accruing to the individual are vast but difficult to perceive, while the government's interest is susceptible to grand characterizations, with vivid examples in the War on Terror era. Moreover, because the judiciary may not be qualified to scrutinize the government's policy justifications, a rubber-stamping of the government's data collection is the likely outcome.

C. Displacing Nixon: NASA as Forming a Sequel

Fortunately, there is a strong argument that the *NASA* Court is tipping the scale away from a balancing test and toward a more holistic approach. While the Court still faces the same conceptual problems described above, a holistic approach allows the Court to better account for these problems and provide a more coherent analysis.

The reasoning in *Whalen* and *Nixon* look very different; *Nixon* clearly invokes a balancing test and Fourth Amendment

---

[108] Aleinikoff, *supra* note 97, at 991 (discussing how balancing undermines our usual understanding of constitutional law as an interpretive enterprise and thereby transforms it into a general discussion of the reasonableness of government conduct).

[109] Strict scrutiny may also fall prey to this criticism, as strict scrutiny is like balancing with a thumb on the scale on the side of the individual's right. This idea was suggested during a conversation with Professor Alex Aleinikoff.

principles, whereas *Whalen* performs a categorical analysis including factors such as the type of disclosure, context and norms. This disparity is likely a major factor fueling the circuit split. However, since *Nixon* followed only a few months after *Whalen*, lower courts could not hold that there was a switch in the Court's approach as a result of either evolving policy or even a changing bench. Thus, *Nixon* clouded the interpretation of *Whalen*, and the lower courts attempted to reconcile the cases. While it is clear that *NASA* did not make broad pronouncements concerning the disparity between its progenitors, the opinion derides *Nixon* in several ways. For one, the terms "outweigh" and "balance" are conspicuously absent from the *NASA* opinion.[110] Secondly, the *NASA* Court describes *Nixon* as "continu[ing] its discussion of Fourth Amendment principles throughout the 'Privacy' section of the opinion," as if to distinguish the *Nixon* analysis from relevant Fifth Amendment principles.[111] Lastly, the *NASA* opinion noticeably mimics *Whalen*'s vagueness and rejects *Nixon*'s precision; Justice Scalia describes this phenomenon as he states that, "[S]urely one vague opinion [*Whalen*] should not provide an excuse for another [*NASA*]."[112]

Moreover, the reasoning in *NASA* can be seen as mirroring that of *Whalen*. In both cases the Court considers whether the individual's data will be disseminated to the public. Considering the question of whether data is safeguarded (whether by the Privacy Act or locked wire fences) can be seen as the Court's proxy for classifying the case as one involving only disclosure to the government or one involving disclosure plus public dissemination. As the Court determines that public disclosures are *not* a part of the government's program and that unwarranted disclosures are unlikely, the Court proceeds to consider only the propriety of revealing the contested data to the government. In *Whalen*, the Court holds that the disclosures are not significantly different from those required under prior law and are not "meaningfully distinguishable" from "a host of other unpleasant privacy invasions" that receiving health care demands.[113] Similarly, the *NASA* Court states, "judicial review of the Government's challenged inquiries must take into account the *context* in which they arise."[114] The Court then stresses that the disclosures are being made to the government in its capacity as

[110] The term "outweigh" appears once, in a footnote describing *Nixon*. It is unclear from where Justice Scalia quotes the term "balance" in his concurrence, as it does not appear in the majority opinion.

[111] NASA v. Nelson, 131 S. Ct. 746, 756 n.8 (2011). Justice Scalia directly states that the case *was* a Fourth Amendment case. *Id.* at 765 (Scalia, J., concurring).

[112] *Id.* at 767.

[113] Whalen v. Roe, 429 U.S. 589, 602 (1977).

[114] 131 S. Ct. at 757 (majority opinion) (emphasis added).

employer and notes that private employers request similar information. Thus, it is possible to read the analyses not as strictly government versus individual with weighed interests on side, but as the Court taking a broader view that classifies public versus government-only disclosures and considers context and norms.

Of course, if the Court is making such a significant jurisprudential decision in its approach to information privacy law, the question arises as to why the Court is not forthright about the change. One reason might be that the Court is wary of committing to a judicial test due to an ongoing struggle with privacy law generally as well as with data interests. Indeed, the *NASA* Court itself states that it is "proceeding with caution" and "leav[ing] broader issues for another day."[115] As discussed above, the confluence of information's various characteristics complicate informational privacy cases. For one, the nonrivalrous and invisible consumption of information can obscure the "invading" aspect of data collection. In addition, the recombinant nature of information works synergistically with the nonrivalrous and invisible consumption of information to make the extent of data privacy invasions incalculable. Indeed, the development of technology permits data to be reused and recombined in unprecedented, seemingly infinite ways. Yet, harms of a constitutional dimension are at stake due to the power differential that information access can create between citizen and state. Owing to these issues, the conceptual problems so poignantly recognizable in a balancing interpretation of the Court's analysis plague the Court. In effect, the Court is at a nascent stage with all of the uncertainty that accompanies early development, and therefore may be proceeding in a hyper-sensitive and timid manner.

Moving forward, conceptualizing *Whalen* without the influence of *Nixon* produces a framework that can account for complex data privacy issues and interests in a significantly different, more promising way. Considering harms such as power differentials between parties and possible data recombination are questionable considerations for the judiciary due to obvious foreseeability, certainty, and commensurability problems. Thus, such considerations are inappropriate in a balancing test where the Court must precisely identify and quantify interests. Fortunately, a different framework can better accommodate these considerations. The alternative reading of *Whalen* is a holistic analysis that does not require quantifying incommensurable interests or pitting the citizen against the state.

The alternative interpretation of *Whalen* and *NASA* accounts for context, reasonableness and norms to provide a categorical

[115] *Id.*

analysis that speaks to principles. In each case the distinction between government and public disclosures classifies the individual's interest, which is then further categorized by the context and type of data. In *Whalen*, only disclosures to the government were at issue and the context involved a) Schedule II drugs, and b) information collected under prior law and typically released in health care situations. In *NASA*, only disclosures to the government were at issue again and the context involved a) federal contractors, and b) information normally collected by private employers. Rejecting a rigid, bifurcated analysis resonates with Michael Chertoff's observation that policies are not always easily classified as pro- and anti-privacy, rather some policies are simply trade-offs on different elements of privacy.[116] The holistic analysis presented above captures data privacy issues at a level that does not reduce the debate to being pro or anti privacy; it captures norms and principles.[117]

At this early stage in the Court's informational privacy case law, there is an opportunity to recognize the complexities of data privacy interests and tailor the doctrine accordingly. Developing a fluid, holistic framework is more demanding than a straightforward weighing of two "opposing" interests. Approaching rights outside of a balancing framework involves thinking of rights as developments, and as the rights crystallize their limitations are embedded within them. This development involves logic, history, values, and constitutional norms.[118] *Whalen* and *NASA* provide an excellent foundation, performing a two-part analysis consisting of a consideration of the breadth and context of disclosure as well as the change from prior norms. Yet, further research is needed to develop informational privacy doctrines within this framework and to provide both substance and meaning to data privacy rights.

---

[116] Michael Chertoff, Secretary, Dep't of Homeland Security, Remarks at the Data Privacy and Integrity Meeting (Mar. 7, 2006), *available at* http://www.dhs.gov/xnews/speeches/speech_0269.shtm. For a discussion of how both individual and government interests can be conceived of in both public and private terms see Aleinikoff, *supra* note 97 at 981. Aleinikoff provides a First Amendment example: an individual interest in communicating one's ideas can be stated as a societal interest in a diverse marketplace of ideas. Furthermore, time, place and manner limitations on expressive behavior can be stated as a government interest in public safety or as a private interest in unencumbered access to public facilities.

[117] Helen Nissenbaum defines contextual integrity as "when informational norms are respected," and describes these norms as "govern[ing] the flow of information about a subject from one party to another, taking account of the capacities (or roles) in which the parties act, the types of information, and the principles under which this information is transmitted among the parties." HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 14 (2009).

[118] This conceptualization of rights was formed during a conversation with Professor Alex Aleinikoff.

Fortunately, privacy interests pervade the Constitution from the First, Third, Fourth, Fifth, Ninth and Fourteenth Amendments, providing principles that will not so much limit, but rather *define* the right to nondisclosure.[119]

CONCLUSION

The Court has continued to struggle with adjudicating a right to informational privacy from its initial foray into this body of law in *Whalen* through its decision in *NASA*. Nonetheless, the Court must confront and engage with constitutional data privacy rights in order to bring coherence and direction to the courts, regardless of how we ultimately value any such right. The Court's struggle can be attributed not only to the complex and multi-faceted nature of privacy generally, but also to the exceptional characteristics of information. Data interests pose particular problems for judges because the nonrivalrous, invisible and recombinant nature of information revolutionizes and intensifies the harm of privacy invasions while at the same time making the harms difficult to detect. Indeed, the harms of data privacy invasions range from misrepresentation of individuals to distortion of the democratic relationship between citizen and state.

This Article argues that the Court's data privacy cases conflict and that *NASA*'s approach to this conflict can be read in two principal ways. The different method of reasoning employed in these two approaches affects the Court's ability to engage with the complex issues data privacy poses. *Whalen*, *Nixon*, and *NASA* can be read as forming a single approach to informational privacy rights, that of a balancing test, or read as consisting of competing approaches with the fluid, holistic analysis ultimately displacing the balancing test. A fluid and holistic understanding of the Court's reasoning conceptualizes the parties' interests in a way that enables the Court to incorporate the parties' interests with all of their

[119] Eugene Volokh makes a similar argument in regards to applying strict scrutiny to the First Amendment. Volokh argues that there should be categorical rules and exceptions based on a theory of the Constitution, stating that:
"By abandoning strict scrutiny of content-based restrictions—or perhaps even intermediate scrutiny of commercial speech restrictions—the Court can shift its focus to creating, as best it can, rules that capture its theory about the proper role of such restrictions. It could, for instance, say that content-based regulations of high-value speech imposed by the government acting as sovereign are simply per se unconstitutional (subject to the recognized exceptions). . . . In each case, the Court would ask the familiar questions: Does some interpretive theory—whether tied to the constitutional text, to broader constitutional or moral values, to the case law, or to something else—support this distinction? Is the proposed rule likely to lead to good results in most cases? Is the rule likely to be properly administered by courts and other government officials?" Eugene Volokh, *Freedom of Speech*, *Permissible Tailoring and Transcending Strict Scrutiny*, 144 U. PA. L. REV. 2417, 2457-58 (1995-1996).

dimensions and complexity into its analysis. Such an analysis closely follows the nature of the disclosure and the context and norms surrounding the disclosure, without placing the parties' interests into a strict, dichotomous relationship. The suggestions presented here for understanding and remedying the Court's data privacy case law are nascent, but identify an opportunity and direction for development to prepare for this "battleground of the future."[120]

[120] David L. Hudson Jr., *Privacy & Newsgathering*, FIRST AMENDMENT CENTER (Sept. 14, 2004), http://www.firstamendmentcenter.org/privacy-newsgathering (quoting Lee Levine).