

2012-2013  
SOUTHERN ILLINOIS UNIVERSITY  
NATIONAL HEALTH LAW MOOT COURT COMPETITION

---

Transcript of Record  
Docket No. 12-1142

Supreme Court of the United States  
October Term, 2012

**HANNAH JASPER, individually and on behalf of  
all others similarly situated,  
Petitioner**

v.

**SPRINGFIELD MUNICIPAL HEALTH &  
WILLIAM DALY, in his individual and official  
capacities as Chief Information Officer,  
Respondents.**

---

---

***COMPETITION PROBLEM***

---

***SPONSORED BY:***

*Center for Health Law and Policy  
Southern Illinois University School of Law*

*Department of Medical Humanities  
Southern Illinois University School of Medicine*

*The American College of Legal Medicine*

*The American College of Legal Medicine Foundation*

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ILLINOIS

HANNAH JASPER, individually and on behalf of )  
all others similarly situated, )  
Plaintiff, )  
 ) No. Civ-11-4523  
v. )  
 )  
SPRINGFIELD MUNICIPAL HEALTH & )  
WILLIAM DALY, in his individual and official )  
capacities as Chief Information Officer, )  
Defendants. )

ROSE HARPER, District Judge

This matter comes before the Court upon motion by Defendants Springfield Municipal Health Clinics and William Daly to dismiss the § 1983 claims brought by the plaintiff class. **Daly was the Chief Information Officer** for the Springfield Municipal Health Clinics (“Clinics”) during two serious and preventable data security breaches involving patient medical records. Plaintiff Hannah Jasper filed this 42 U.S.C. §1983 action on her own behalf and on behalf of all other similarly situated patients of the Springfield Municipal Health Clinics who received care at the clinic between January 1, 2003, and October 16, 2009, based on alleged violations of their **constitutional** right to privacy. She seeks **injunctive** relief against the Clinics and Daly in his official capacity, and **money** damages against Daly in his individual capacity. Defendants assert that Plaintiff has failed to state a claim upon which relief may be granted because there was no constitutional right at stake here; Defendant Daly additionally argues he is entitled to qualified immunity in his individual capacity, and both Defendants assert there was no municipal custom or policy, as required for § 1983 liability against the Clinics. Both

Defendants further assert that this matter is not appropriate for class action status because individual issues will predominate.

Because both parties have submitted affidavits from expert witnesses that go beyond the pleadings in the case, the Court will treat this as a motion for summary judgment. For the reasons set forth below, Defendants' motion is GRANTED because the Court finds Plaintiff has failed to allege a violation of her constitutional rights. The Court concludes it is not necessary to address the remainder of Defendants' objections given the resolution of the underlying constitutional claims.<sup>1</sup> *See Pearson v. Callahan*, 555 U.S. 223, 238 (2009) (giving courts discretion whether to address underlying constitutional issues as an initial matter in § 1983 claims).

## **I. Facts**

The parties largely agree on the facts. Where there is ambiguity, it is resolved here in favor of plaintiff Jasper, the non-moving party. *Jesinger v. Nev. Fed. Credit Union*, 24 F.3d 1127, 1130 (9th Cir. 1994). The city of Springfield operates six municipal health clinics in an effort to make primary healthcare services available to all residents. The clinics perform a full range of non-emergency healthcare services including family planning, monitoring of chronic illness, post-hospital rehabilitation, testing for sexually-transmitted diseases, and blood and urine exams, as well as less sensitive services such as dental care. Defendant Daly was the Chief Information Technology director for the Springfield Municipal Health Clinics ("Clinics") from 2007 until recently. His

---

<sup>1</sup>The Court finds that there are factual issues that would in any event preclude summary judgment at this stage, both as to the § 1983 claims (concerning the Clinics' policies and the scope of Daly's involvement) and the class certification.

professional responsibilities included the management of the Clinics' information systems and the security of the Clinics' patient health data.

On February 2, 2009, under Daly's leadership, the Clinics began using new electronic medical records software called SpaceMed. The software is designed to both manage patient files for those authorized to access them and to secure the health data from unauthorized intrusions. The Information Technology (IT) department successfully transferred to SpaceMed the files of all patients who had visited any of the Clinics' offices since January 1, 2003. Daly was careful to instruct all clinic physicians and staff about the creation of strong passwords, consisting of at least 8 characters and including at least one number and one capital letter, for their user accounts to the SpaceMed software. However, Daly failed to change the default password for the system administrator's account. Consequently, on February 14, 2009, a hacker was able to breach the Clinics' data security using the default password "password." Though the hacker was never identified, he or she appears to have broken into the Clinics' system only for the purpose of making a demonstration attack. The hacker, a self-described "hactivist," revealed the details of the attack to a prominent technology blog journalist, purportedly in the hopes that security would be improved. Because the hacker was able to log in as the system administrator, he or she had more privileges than a physician would have; the system administrator account allows not only access and modification, but wholesale copying and deletion of the master file of patient records.

The Clinics issued a public apology, and Daly changed the system administrator password. Unfortunately, the security was short-lived. Very early on the morning of October 17, 2009, the Clinics' servers sustained another attack. This hacker again

accessed patient health data through the system administrator account, but this time, the attack had the trappings of a malicious hack. The unauthorized intruder downloaded and deleted the files from the Clinics' servers. An outside data security consulting firm was called in immediately upon discovery of the breach. The consulting firm's investigation concluded that at the time of the second hack, the system administrator account's password had been set to "11111." Although there is some disagreement in the record over when the weak password was in use, Daly does not dispute that he was responsible for setting the admin password and did in fact set it.<sup>2</sup> The Clinics retained a backup copy of all of the deleted health files and were able to restore their information systems quickly. To date neither the Clinics, patients, nor law enforcement authorities know the identity of the hacker or how the medical files have been used.

## II. 42 U.S.C. §1983

Plaintiff filed suit against the Springfield Municipal Health Clinics and William Daly on behalf of all patients of the Clinics whose medical records were downloaded by the unidentified hacker on October 17, 2009. The claim is brought under 42 U.S.C. §1983. To prevail under section 1983, the plaintiffs must prove that they were "deprived of a right secured by the Constitution or laws of the United States, and that the alleged deprivation was committed under color of state law."<sup>3</sup> *Am. Mfg. Mut. Ins. Co. v. Sullivan*,

---

<sup>2</sup>Daly explained that because others in the IT department also use the system administrator account, he wanted to set something easy to remember for the time being, and then come back and set a more secure password when there was more time. He then simply forgot to do so. The consulting firm noted that besides these two hacks on patient records, the Clinics had someone hack into the employee email system about three months prior, also through a system administrator account. The consulting firm concluded the Clinics' security systems had several areas of critical inadequacy.

<sup>3</sup>Defendant Daly concedes that the conduct in this case was performed while he was a government official, so state action is not at issue.

526 U.S. 40, 49-50 (1999). Plaintiffs argue that defendant Daly violated their constitutional right to privacy by neglecting to protect their sensitive health information.<sup>4</sup>

### **A. THE SUBSTANTIVE DUE PROCESS RIGHT TO PRIVACY**

This is the first claim based on a constitutional right to information privacy in this circuit. The Supreme Court’s precedent on the matter has been vague and infrequent, and the interpretations from our sister circuits are inconsistent, to say the least. The right to information privacy can only be found in the “penumbra” of the United States Constitution and enforced through the Fifth and Fourteenth Amendments’ protections of substantive due process. There are precisely three U.S. Supreme Court opinions that address the right to information privacy, and in all three the parties relying on the right have lost.

The U.S. Supreme Court recognized the right for the first time in *Whalen v. Roe*, when it analyzed the constitutionality of a New York statute requiring pharmacies to report prescription information related to highly addictive pharmaceutical drugs to the New York State Department of Health. 429 U.S. 589, 591 (1977). The Court considered whether New York’s reporting program impinged on either of two distinguishable types of privacy interests: decisional autonomy of the sort implicated by *Griswold v. Connecticut*, 381 U.S. 479 (1965), or informational privacy of the sort at issue in this case. *Whalen*, 429 U.S. at 599-600. The Court determined that the New York statute did not pose a “sufficiently grievous threat” to raise constitutional concerns. *Id.* at 600.

---

<sup>4</sup>Plaintiffs’ original complaint also alleged Defendants’ failure to comply with the security provisions of the Health Insurance Portability and Accountability Act (“HIPAA”), 42 U.S.C. § 1320d-1320d-9. Plaintiff subsequently dropped this claim because HIPAA creates no private right of action, either on its own or through section 1983. *See United States v. Streich*, 560 F.3d 926, 935 (9th Cir. 2009).

Later the same year, the Court rejected President Nixon's constitutional privacy challenge to the Presidential Recordings and Materials Preservation Act, a law that mandated public access to most (but not all) of President Nixon's audio tape recordings produced during his presidency. *See Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425 (1977). Because the statute directed the archive administrator to return all of President Nixon's tape recordings that were purely personal and unrelated to his presidency to him, the Court found that the Act struck a balance between the public's interest in oversight of public officials and President Nixon's interests in his purely private information. *Id.* at 459. At the same time, the opinion avoided confirming the existence of a constitutional interest in information privacy by stating only that the Court "may agree" the right exists, and "may assume" that the President has expectations of privacy in his tape archive. *Id.*

The third and last time the high court addressed a constitutional interest in the avoidance of disclosure of personal matters occurred just last month in *NASA v. Nelson*, 131 S. Ct. 746 (2011). *NASA* has the virtue of being recent, but it adds little for our purposes. The Court under the facts of that case merely "assumed without deciding" that the Constitution protects information privacy rights. *Id.* at 751. The Court found that the government's interest in collecting and maintaining the information in question outweighed the plaintiff's interests in non-disclosure. *Id.* at 762.

None of the constitutional challenges that have made it to the Supreme Court have addressed a scenario like this one, where the alleged constitutional foul is a particular incident of a government *re-disclosure*. As the *NASA* opinion points out, the Supreme Court precedents have addressed prospective challenges to the government's plan to collect personal information. *Id.* The plaintiffs in this case do not challenge the initial

collection of their health information—indeed, they were willing patients at a public health clinic. Instead they challenge the acts and omissions that caused the Clinics to make an unanticipated disclosure of their records to a third party.

The Supreme Court has not settled on privacy's place in the fabric of our Constitution, so guidance must come from the fractured and contradicting approaches taken by our sister circuits. Generally speaking, when federal courts outside this circuit assess asserted violations of constitutional confidentiality, they apply one of two rules: the more privacy-protective balancing of interests test developed in the Third Circuit and embraced by most of the others, or the less protective test developed by the Sixth Circuit.

In *United States v. Westinghouse Electric Corp.*, the Third Circuit declared that the constitutional right to confidentiality must balance the privacy interests of the individual against the competing interests of the state. 638 F.2d 570, 578 (3d Cir. 1980) (outlining several factors that must be balanced). The *Westinghouse* court started from the position that people have a constitutional interest in their health records because “information about one’s body and state of health is matter which the individual is ordinarily entitled to retain within the ‘private enclave where he may lead a private life.’” *Id.* at 577 (quoting *United States v. Grunewald*, 233 F.2d 556, 581-82 (2d Cir. 1956)).

On the other hand, the Sixth Circuit declined to embrace so broad a conception of privacy. See *J.P. v. DeSanti* 653 F.2d 1080, 1090 (6th Cir. 1981). The Sixth Circuit’s vision for privacy served the narrow purpose of preserving rights that “can be deemed ‘fundamental’ or ‘implicit in the concept of ordered liberty.’” *Id.* Accordingly, the Sixth Circuit only recognizes the right when the privacy interests are inexorably linked to a fundamental right. For example, that court found a privacy right of constitutional

dimension in the personnel files of undercover police officers that protected those officers from disclosure of that information to defense counsel representing a violent gang, because it “created a very real threat to the officers’ and their family members’ personal security and bodily integrity, and possibly their lives.” *Kallstrom v. City of Columbus*, 136 F.3d 1055, 1063 (6th Cir. 1998). The Sixth Circuit’s rule for constitutional privacy claims has come to be known as the “state-created danger” doctrine. *See Barber v. Overton*, 496 F.3d 449, 453 (6th Cir. 2007) (describing Sixth Circuit rule).

Given the high court’s reluctance to define or recognize the right to information privacy, and Justice Scalia’s recent persuasive exposition in his *NASA* dissent that it ought not exist at all, this Court is convinced that the Sixth Circuit’s state-created danger test is the most appropriate.

## **B. ANALYSIS**

Plaintiffs’ claim quite obviously falls short of the threshold for state-created danger. Plaintiffs would have to show that the disclosure of their sensitive health information put them at immediate risk to their personal security or some other fundamental liberty. The Sixth Circuit has found this to be the case only in certain exceptional contexts. *See, e.g., Moore v. Prevo*, 379 Fed.Appx. 427, 740 (6th Cir. 2010) (finding disclosure of a prisoner’s positive HIV status to other inmates did put prisoner at sufficient risk). Ordinary leaks of health data do not raise constitutional concerns.

Plaintiffs do not, and cannot, articulate a harm to physical security that is likely to result from the two security breaches sustained by the Clinics. Though the Plaintiffs attempt to speculate about various misuses of their medical information—identity theft, targeted advertising, and even shaming campaigns—even if the Court were to accept that

these highly speculative harms might come to pass, they do not interfere with the Plaintiffs' physical safety or fundamental liberties.

Just as the screening questionnaires in *NASA* were found to be too pervasive to be of constitutional significance, the amassing of large quantities of health data—even highly personal data on HIV status and pregnancy—is now the norm. The occasional unintentional lapse in security is also commonplace. Where the Plaintiffs suffer mere indignities and inflated fears of future consequences, constitutional rights have not been implicated. As *Whalen* states, “disclosures of private medical information...are often an essential part of modern medical practice even when the disclosure may reflect unfavorably on the character of the patient.” *Whalen*, 429 U.S. at 602.

### **III. CONCLUSION**

Even assuming the facts and inferences in her favor, Plaintiff has simply failed to allege any facts that implicate her constitutional rights to information privacy. Because Plaintiff has failed to state a constitutional claim upon which relief can be granted, her claims should be dismissed.

### **ORDER**

Defendants' motion is GRANTED.

IT IS SO ORDERED.

---

Rose Harper, District Judge  
February 28, 2011

IN THE UNITED STATES COURT OF APPEALS  
FOR THE TWELFTH CIRCUIT

No. 12-344

HANNAH JASPER, individually and on  
behalf of all others similarly situated,  
Appellant,

v.

SPRINGFIELD MUNICIPAL HEALTH  
CLINICS & WILLIAM DALY, in his individual  
and official capacities as Chief Information Officer,  
Appellees.

Appeal from the United States Federal Court for the District of Illinoza,  
Case No. Civ-11-4523—Rose Harper, District Judge

Argued May 31, 2012 – Filed July 2, 2012

Before: Bryson, Decker, Van Halenburg, Circuit Judges.

Van Halenburg, Circuit Judge:

Appellant in this action is a patient of the Springfield Municipal Health Clinics (“Clinics”) whose health records were left insecure during two incidents of unauthorized access to the Clinics’ servers. On behalf of a class of individuals similarly situated, Appellant filed a section 1983 lawsuit against the Springfield Municipal Health Clinics and William Daly, the Chief Information Officer of the Clinics, on the theory that Daly’s failure to secure the Clinics health records violated the class’s constitutional right to privacy. The Federal District Court for the District of Illinoza granted Appellees a summary judgment, concluding that their alleged conduct did not implicate Appellant’s right to privacy.

We agree with the holding of the district court, but for a wholly different reason.<sup>5</sup> We find that health records are the quintessential example of private information deserving protection from unnecessary disclosure, and that Appellant undoubtedly had a privacy interest of constitutional magnitude. However, because Appellees' conduct was unintentional, the disclosures in this case do not meet the standard for "egregious" behavior required to show a deprivation of substantive due process. Thus, we sustain the district court's decision to grant summary judgment in favor of Appellees.

### FACTS

Most of the relevant facts are set out in the district court's opinion, and we decline to make a redundant account of the record here. The only facts we are inclined to add to the district court's thorough account are those from the affidavits of the parties' expert witnesses, both of whom are computer security experts. The affidavits reveal that the two hacking attacks at issue in this case are very common. The first attack was likely a password-guessing attack, and the second may have been a brute-force attack.

As the name implies, a hacker attempting a password-guessing attack will try a few common default passwords, such as "password," or commonly chosen weak passwords, such as street names and birth dates, in the hopes that a user has assigned a predictable password to his or her account.

A brute-force attack, by contrast, is an attempt to discover a password by systematically trying combinations of letters, numbers, and symbols until one of them works. Any website or web-based system that requires user authentication can be a target

---

<sup>5</sup>We agree with another aspect of the district court opinion, namely that factual issues would need to be resolved before that court could rule on Appellees' challenges to § 1983 liability and the status of the plaintiff class, and for similar reasons, we will not address those issues.

for a brute-force attack, but the system can be designed to significantly reduce the risk that an attack will work. First, if the passwords are strong enough (that is, complex enough), a computer program that continuously tries new combinations of letters and numbers can take years to succeed. For example, the Clinics' physicians and staff were instructed to create passwords that contained at least eight characters including both upper-case and lower-case letters and at least one number. There are over 200 trillion unique strings of eight characters using these rules. On the other hand, there are only 100,000 unique strings of five numbers. The experts agree that Appellee Daly's choice of password "11111" was very weak because it was vulnerable to both password-guessing and brute-force attacks.

Appellant also claims that Daly could have and should have programmed the SpaceMed program to lock accounts after several successive attempts to login have failed in order to thwart brute-force attacks. Appellees respond that this setting would make the Clinics' system vulnerable to "denial of service" attacks. These are attacks designed to shut authorized users out of the system, and can potentially cause problems in the provision of care by staff and physicians at the Clinics.

## **DISCUSSION**

Because the district court resolved this case at the summary judgment phase, we review the opinion de novo. *Horton v. Reliance Std. Life Ins. Co.*, 141 F.3d 1038, 1040 (11th Cir. 1998).

### **I. Constitutional Interest in Non-Disclosure**

As the district court noted, *Whalen v. Roe*, 429 U.S. 589 (1977), recognized a constitutional right to privacy in personal information. This right is often referred to as

the “confidentiality branch” of privacy to distinguish it from the privacy rights in autonomy and independence of decision-making. *See, e.g., Doe v. City of New York*, 15 F.3d 264, 267 (2d Cir. 1994) (“There is [] a recognized constitutional right to privacy in personal information. More precisely, this right to privacy can be characterized as a right to ‘confidentiality,’ to distinguish it from the right to autonomy and independence in decision-making for personal matters also recognized in *Whalen*.”).

The district court noted the timidity with which the Supreme Court has created and defined the right to constitutional confidentiality, and, on that basis, elected to use the Sixth Circuit’s “state created danger” test because it is the most limited. Though we understand the district court’s cautious approach, we disagree with the Sixth Circuit’s rule. The facts and reasoning in *Whalen* belie the Sixth Circuit’s approach, and show that the state-created danger rule is under inclusive. The Court found that the security precautions in the New York statute at issue in *Whalen* were a determinative factor against finding a constitutional violation—if the Sixth Circuit’s state-created danger test really were the law of the land, those security precautions would have been irrelevant. All that would have mattered is that the revelation of prescription use to the public at large did not put the patients in immediate peril or threat of physical insecurity.

We therefore agree with the majority of our sister circuits that a constitutional interest in information privacy should be determined based on a more nuanced multi-factor test that takes into account the sensitivity of the information at hand and the competing reasons for collection and disclosure. *See, e.g., U.S. v. Westinghouse Elec. Corp.*, 638 F.2d 570, 578 (3rd Cir. 1980) (concluding court must “engage in the delicate task of weighing competing interests”). This constitutional interest is surely implicated

when patients' health records are exposed to third parties for no legitimate purpose. *See Doe v. City of New York*, 15 F.3d 264, 267 (2d Cir. 1994) (finding "few matters are quite so personal as the status of one's health"). The Supreme Court has not, however, clearly deemed this interest to be fundamental, and we do not do so today, finding it unnecessary to reach the conclusion Appellant has a protected privacy interest at stake here.

Like the plaintiffs in *United States v. Westinghouse Electric Corp.*, Appellant in this case had a strong interest in keeping her detailed health histories confidential. 638 F.2d 570, 577 (3d Cir. 1980). Unlike the defendant in *Westinghouse*, who wished to release the health records to researchers to facilitate an important public health study, the disclosure in this case served no compelling public interest whatsoever. *See id.* at 576. Thus, in this case, the balance falls squarely on the side of Appellant.

Our conclusion is consistent with countless precedents in other jurisdictions finding constitutional confidentiality interests in other contexts. *See, e.g., Denius v. Dunlap*, 209 F.3d 944, 956 (7th Cir. 2000) (complete medical records); *Sheets v. Salt Lake County*, 45 F.3d 1383, 1388 (10<sup>th</sup> Cir. 1995) (a diary); *Marsh v. County of San Diego*, 680 F.3d 1148, 1152 (9th Cir. 2012) (autopsy images); *but see Riley v. St. Louis County of Mo.*, 153 F.3d 627, 630-31 (8th Cir. 1998) (coming to the opposite conclusion about photographs of the corpse of a gang member).

## **II. Egregiousness of Appellee's Conduct**

Our finding that Appellant had a constitutional interest in the confidentiality of her health records does not end our inquiry. The Court has emphasized that substantive due process protects citizens against arbitrary government action, and "only the most egregious official conduct can be said to be 'arbitrary in the constitutional sense.'"

*County of Sacramento v. Lewis*, 523 U.S. 833, 846 (1998) (quoting *Collins v. Harker Heights*, 503 U.S. 115, 129 (1992)). In other words, due process guarantees are violated only through egregious acts. Claimants must be prepared to prove culpability of the state actor that goes well beyond negligence. The state actor must have engaged in conduct “that shocks the conscience or interferes with rights implicit in the concept of ordered liberty.” *United States v. Salerno*, 481 U.S. 739, 746 (1987) (citing *Rochin v. California*, 342 U.S. 165, 172 (1952)).<sup>6</sup>

In *Daniels v. Williams*, the Supreme Court found that a prison custodian’s failure to remove a pillow on the prison stairs could not be the basis for a deprivation of substantive due process because it was mere negligence. 474 U.S. 327, 328 (1986). In *County of Sacramento v. Lewis*, the Court concluded that a police officer’s conduct in conducting a high speed chase of a suspect on a motorcycle, whose passenger was then struck and killed by the police car, also could not be the basis for a substantive due process claim because the standard of culpability in such circumstances required an intent to cause harm, not merely deliberate indifference or recklessness. 523 U.S. 833, 854 (1998).

After *Lewis*, our sister circuits have adopted varying approaches regarding what level of culpability is required in order to meet the requisite standard. *See generally*, Rosalie Berger Levinson, *Time to Bury the Shocks the Conscience Test*, 13 Chap. L. Rev. 307 (2010). A few courts have read *Lewis* to suggest that when there is a fundamental right at stake, it is not necessary to show the conduct also shocks the conscience. *See id.* at 307-08. Other circuits, however, have applied the shocks the conscience test

---

<sup>6</sup>This issue of culpability relates to the underlying constitutional standard at issue, an inquiry separate from whether there is liability under § 1983.

regardless, including cases involving informational privacy. *See O'Connor v. Pierson*, 426 F.3d 187, 203 (2d Cir. 2005). We think the latter approach most appropriately melds the scope of the right suggested by *Whalen* with the Supreme Court's concerns about the breadth of substantive due process law, and we will require Appellant to show that Appellees' conduct here shocks the contemporary conscience.

Under that test, the circuits also disagree whether actions that are deliberately indifferent or reckless can "shock the conscience," or whether specific intent to harm is always required. Levinson, *Conscience Test*, *supra*, at 325. Again, we don't feel the need to resolve that issue definitively, because even assuming the conduct in this case was deliberately indifferent to Appellant's rights, that conduct simply wasn't egregious enough to shock the contemporary conscience. No one would think Daly did his job well or even competently. Appellees should have protected the sensitive health information of the Clinics' patients better than they did. But they did not purposely disclose the health records to the hackers, and they did not exhibit any malice toward Appellant.

Technically, in fact, they did not disclose anything—the hacker did.

Our dissenting colleague argues that information privacy is different from other substantive due process rights because the state has an affirmative duty sourced in the Constitution to provide adequate security. Judge Decker points to language in *Whalen v. Roe* to further the argument. We disagree with this interpretation of the precedent. Though the Court in *Whalen* did suggest that New York's plan to provide security to the prescription information collected by the state was an important factor in its analysis of the constitutionality of the program, the existence of a program and commitment to avoid unwarranted disclosures was alone sufficient to discharge this. *See Whalen*, 429 U.S. at

605. The Court did not say that the program needed to be infallible. Moreover, in *NASA v. Nelson*, the Supreme Court explicitly rejected the notion that the government must use the least restrictive means of furthering its interests when privacy is at stake. 131 S. Ct. 746, 760 (2011).

Judge Decker laments that *Lewis* constrains our power to recognize new facets of substantive due process, but however one may feel about *Lewis*, this case makes an excellent cautionary tale against the reflexive impulse to constitutionalize every perceived slight and indignity. The ubiquity of data spills and data breaches, while not ideal, has proven to be relatively harmless as far as human rights are concerned. The district court noted this when it wrote about the “pervasiveness” of the large accumulations of health data.

The Clinics, though publicly run, did not have the sort of relationship with Appellant that leveraged any unique and formidable powers possessed by state actors. The only difference between the data breaches in this case and the hundreds of others is that this one happened to take place on the servers of a public entity. A constitutional claim of this sort would be a perversion of the Fifth and Fourteenth Amendments, and we will not allow it.

AFFIRMED.

Decker, J., concurring and dissenting:

I concur with the majority’s analysis in Part I, adopting the *Westinghouse* multi-factor test of information privacy and concluding Appellant has a privacy interest in the security of her health records. However, I respectfully dissent from the analysis in Part II. Because Appellees failed to provide the most basic security for Appellant’s sensitive

health records, their conduct “shocks the conscience.” I would reverse the district court’s summary judgment ruling.

### **I. Mental State Requirement for Deprivation of Substantive Due Process**

The majority makes much of the fact that Appellees “did not disclose anything,” and believes this saves Appellees from a finding that their conduct was egregious. This relies too heavily on an untenable act/omission distinction, and looks too narrowly in time and space at the point of disclosure. The Court is free to look more broadly for conduct that touches on Appellant’s constitutional rights. A disclosure might not be necessary; the Third Circuit has found that a *threat* to disclose private information about a youth’s sexuality can constitute a deprivation of privacy, even though there had been no actual disclosure. *Sterling v. Borough of Minersville*, 232 F.3d 190, 197 (3d Cir. 2000).

In any event, Daly did engage in an intentional, egregious act when he reset the system administrator password to “11111.” This action produced a false sense of security. The majority’s reliance on the illegal acts of third parties is also unpersuasive. The expert affidavits from both parties confirm the ease and frequency of brute force attacks on information systems. Since hacking attacks of this sort are so common, Daly’s conduct is not meaningfully different from publishing the records on the Internet for a period of time.

The majority also makes too much of the mental state requirement. A case just decided by the Ninth Circuit is instructive. In *Marsh v. County of San Diego*, a retired district attorney disclosed autopsy photographs of the corpse of the plaintiff’s young son to a local newspaper and television station along with a memo, titled “What Really Happened to Phillip Buell?,” describing the retired prosecutor’s thoughts on a child abuse

conviction that had later been thrown out. 680 F.3d 1148, 1152 (9th Cir. 2012). The court found that this disclosure shocked the conscience and violated the mother’s substantive due process rights in privacy and sepulchre. *Id.* at 1155. The court did not claim the district attorney had the specific intent to interfere with the family’s grief or to disturb their privacy; rather, the inevitable consequences of the district attorney’s actions were egregious enough. *See id.* (finding the defendant’s actions “degrade[d] the respect accorded to families in their time of grief”). In reaching its holding, the court in effect focused on the most important of the *Westinghouse* factors—the countervailing interests in disclosure. Because the district attorney disclosed the photographs “without any legitimate governmental purpose,” the analysis was easy. *See id.*

It is easy in our case, too. Appellees had no legitimate reason to expose the Clinics patients’ health information to an unknown hacker. In fact, this disclosure is far less legitimate than the disclosures in *Marsh*, where the district attorney evidently believed the photographs were pertinent to a public debate about the death of a child who may have been the victim of child abuse. The disclosure of Appellant’s health information is an unambiguous, wholly harmful event with no countervailing benefits.

## **II. Affirmative Duties to Secure Personal Information**

The majority reads *County of Sacramento v. Lewis*, 523 U.S. 833 (1998), and *Daniels v. Williams*, 474 U.S. 327 (1986), to mean that nothing less than intentional acts can ever be the basis for a violation of substantive due process. In doing so, the majority fails to heed *Lewis*’ acknowledgement that municipal liability under §1983 rests on acts of deliberate indifference. *See Lewis*, 523 U.S. at 850 n. 10. Even as to Appellee Daly individually, this understanding divorces the *Lewis* and *Daniels* opinions from the

contexts in which they were decided, which were starkly different from this case. *Lewis* involved a police chase, and *Daniels* involved inadvertent injury to a prisoner. *Parratt v. Taylor*, the case that *Daniels* overruled, addressed the inadvertent loss of the tangible property of a prisoner. *See Parratt*, 451 U.S. 527, 529 (1981). In all these cases, the rights of Americans are negative rights—the right *not* to suffer physical interference with our bodies, life, and property. The majority forgets that the Supreme Court’s decision in *Whalen* recognized an affirmative duty on the government’s part to provide security for personal information in the government’s possession. *Whalen*, 429 U.S. at 605-606.

The Supreme Court’s decision in *Whalen* was dependent on the state of New York’s plan to secure the data from breach or spill. The Court specifically stated that the outcome of the case might be different without adequate security. *Id.* Before the case at bar, while no federal courts have had the opportunity to opine on the constitutional implications of lax, reckless data security, they have frequently acknowledged that data security is a prerequisite for constitutional information collection. *See, e.g., Gen. Motors Corp. v. Dir. of Nat’l Inst. Occupational Safety and Health*, 636 F.2d 163 (6th Cir. 1980) (finding that a subpoena for employee medical records is enforceable under *Whalen* because of the protections against public disclosure); *see also Greenville Women’s Clinic v. Comm’r, S.C. Dep’t of Health*, 317 F.3d 357 (4th Cir. 2002) (concluding that South Carolina’s abortion clinic recordkeeping regulation, which required said records be open to public health inspection, wasn’t a *per se* violation of patient privacy but that adequate protections against unwarranted disclosure were necessary to keep the program within the bounds of the Constitution).

Appellees in this case failed to mitigate the potential for disclosure. When the patient's complete set of medical records are separated from the world only by the password "11111," the patients have been deprived of the security guaranteed by the Constitution. The majority has simply overreacted to the cautionary tone of *Lewis* and *Daniels*.

*Whalen* went to great lengths to address the privacy concerns of many Americans as our personal data accumulates on countless computers and servers. These anxieties are not misplaced; the Privacy Rights Clearinghouse reports over 700 breaches of health records since 2005, affecting over 20 million individual records. See *Chronology of Data Breaches*, Privacy Rights Clearinghouse, <http://www.privacyrights.org/data-breach/new> (last visited July 1, 2012). Our faith in technology and efficiency comes at the price of lost control over our most personal information. Believing that this price would be too great without appropriate security measures, the *Whalen* Court singled out data security as a constitutional requirement, and reserved analysis of the contours of that duty for another day. This Circuit now abdicates its responsibility to do so.

By contrast, the Ninth Circuit has not. *Marsh* recognized and respected the inchoate harms that make privacy such a unique, hard, and thoroughly modern problem. Though there was no suggestion that gruesome autopsy photographs of the plaintiff's son were actually disseminated broadly in that case, the Ninth Circuit understood the plaintiff's fear that it might be disseminated in the future as "not unreasonable" in the age of the Internet. *Marsh*, 680 F.3d at 1155. The majority is keen to point out that Appellant cannot point to any fully realized harm from this security breach. It is possible she never will, even if the breach does in fact affect her life (and the lives of all members

of the class she represents) in pernicious but undiscovered ways.<sup>7</sup> But a search for concrete harms misses the point of privacy law. It is the natural fear of the unknown consequences that makes the loss of privacy capable of “mental pain and distress, far greater than could be inflicted by mere bodily injury.” Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 196 (1890).

I would reverse the district court’s summary judgment order, and remand to the district court for consideration of Appellee’s qualified immunity claim.

---

<sup>7</sup>As noted by the court below, the relief Appellant seeks includes **injunctive relief**, presumably to require the Clinics to adopt appropriate security measures to safeguard her records, which are still in the Clinics’ possession and control, in the future.

Supreme Court of the United States

Hannah Jasper,  
individually and on behalf of all others  
similarly situated, Petitioner

v.

Springfield Municipal Health Clinics  
& William Daly, in his individual  
and official capacities as  
Chief Information Officer, Respondents.

Docket No. 12-1142

ORDER GRANTING CERTIORARI

Petition for writ of certiorari to the Twelfth Circuit Court of Appeals is GRANTED limited to the following Questions:

1. Is there a constitutional right to confidentiality in patient medical records maintained by a municipal government, and if so, what is the scope of that right?
2. Can the inadvertent release of private patient medical records violate the patient's rights of substantive due process?

IT IS SO ORDERED.

Date: July 16, 2012