FILED
November 22, 2021
released at 3:00 p.m.
EDYTHE NASH GAISER, CLERK
SUPREME COURT OF APPEALS
OF WEST VIRGINIA

No. 21-0095 – *State of West Virginia ex rel. West Virginia University Hospitals – East, Inc., doing business as Berkeley Medical Center; City Hospital, Inc., doing business as Berkeley Medical Center; and The Charles Town General Hospital, doing business as Jefferson Medical Center v. The Honorable David M. Hammer, Judge of the Circuit Court of Jefferson County, and Deborah S. Welch and Eugene A. Roman, individually and on behalf of all others similarly situated*

Justice Hutchison, dissenting, and joined by Justice Wooton:

I dissent because neither the record nor the law support the issuance of a writ of prohibition.

Because of the proliferation of data breaches, the law is rapidly evolving on the question of whether plaintiffs, whose data has been stolen, have sufficiently pleaded an injury-in-fact. As one federal judge noted, "[t]here are only two types of companies left in the United States, according to data security experts: 'those that have been hacked and those that don't know they've been hacked.'" *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359, 360 (M.D. Pa. 2015).

The majority opinion has done a disservice to the people of West Virginia and impaired their ability to pursue relief when their data is stolen from a hospital's computer system by a hospital employee. The majority opinion's factual conclusions in support of their legal conclusions set this State apart from just about every other jurisdiction in the nation that has addressed the issue of data breaches.

First, I am troubled that the majority opinion sidestepped the 1,642-page record and, instead, cherry-picked a handful of facts "primarily from the circuit court's findings of fact contained in its order granting class certification."[1] The majority opinion focuses on the notion asserted by West Virginia University Hospitals—East, Inc. ("WVU Hospitals"), that Angela Roberts ("Angela") "legitimately accessed" the data of approximately 7,445 patients in the last 8 months of 2016. Looking at the facts through the hospital's rosy lens, the opinion paints a picture of a blameless hospital victimized by a lone employee.

The majority opinion recites, but then artfully dodges, Angela's admission that she looked at every patient's account with *a dual purpose*: legitimate work *and to steal data* for her boyfriend, Wayne Roberts ("Wayne"). Angela as an employee was an agent of her master and employer, WVU Hospitals; thus, everything Angela did she did in the position of the hospital. In her deposition, Angela admitted that the patient files she "looked at every day were all . . . potential victims." Angela said that even though she "looked at everybody's records for the legitimate purpose, the business purpose," she was also "looking at those records at the same time for an illegitimate purpose and that is to take names and addresses and Social Security numbers for Wayne[.]" When Angela looked at a patient's computer record, she always asked herself if the patient "had enough information on their accounts" and, if so, she would "get their info . . . for Wayne."

[1] ___ W.Va. at ___, ___ S.E.2d at ___ (Maj. Op. at 2).

By sidestepping the facts as they are in the record, the majority opinion misses that Angela designed her movements to conceal her criminal activity. Angela was successful because WVU Hospitals carelessly created and operated a system that permitted her to steal patient data at will. Angela admitted she did not access patient accounts "willy nilly," "this account here, that account there." Angela said she stole the information from "accounts that I was legitimately in for whatever reason," and she did so to avoid raising suspicion by WVU Hospitals, "[s]o if they saw . . . you would see where I scheduled something for that patient or a note from me that I, you know, did something on that account." Most importantly, Angela never thought she would get caught because "nobody was watching me closely enough to know that I was doing anything other than my job." The hospital's failure to monitor its employees' conduct is apparent by the hospital's admission it only became aware of the data breach when it learned of the FBI's investigation of Angela and Wayne.[2]

Simply put: Angela testified that she reviewed patient records with both "a [legitimate] business and a Wayne's business . . . need of looking at all that material[.]" Angela started out looking at each patient's file with a legitimate purpose; she ended by scribbling down the patient's private data or printing out copies of their driver's license or Social Security card. She then gave that information to Wayne, knowing he used it for a

[2] Angela testified in her deposition that her supervisors never monitored her work. Angela said, despite working in an open cubicle, that no one was ever looking over her shoulder. The only time Angela saw or spoke to a supervisor was when Angela left her cubicle and went to her supervisor's office.

criminal purpose. Every one of the 7,445 people, whose patient records were undisputedly accessed by Angela, can say their personal data was invaded for a wrongful purpose and that they were harmed, in part because of Angela's criminal conduct, but also because WVU Hospitals did nothing to stop Angela. The record shows that, if the police had not executed a search warrant on Wayne's apartment (for a wholly unrelated case) and found the yellow scraps of paper with Angela's handwriting of patient data, she never would have been stopped. Angela testified that WVU Hospital's management system was so slipshod that she suspected her other coworkers in nearby cubicles were probably also stealing data, and that no one would have found out.

Second, even if we accept the majority opinion's view of the facts as correct, it does not support its legal conclusion. The majority opinion contends that Angela was "legitimately" looking at patient files when she took the patient's private information, and then draws the conclusion that the patients never suffered an injury-in-fact sufficient to confer standing to bring a class action suit. I think, if you asked the patients whether they feel they suffered an "injury" such as embarrassment, fear of identity theft, or the cost of paying for identity theft protection, they would offer a different answer.

What is more, I think the record supports a finding that patients suffered an injury-in-fact caused by WVU Hospital's carelessness. Angela opened up a patient's file for a legitimate purpose, but before she closed it, she searched the file to steal the patient's identity and WVU Hospitals did nothing to prevent her from doing so. Angela walked out of the hospital with notes and printouts from patient files which she gave to Wayne so he

could engage in various felonies. Let's be clear: what Angela and Wayne did was sufficient to warrant a 36-count federal indictment.[3] For instance, the indictment alleged that Wayne and Angela:

> Devised a scheme and artifice to defraud a financial institution, through which [Wayne] intended to obtain approximately $8,000 from Wells Fargo.
>
> It was a part of the scheme and artifice that the defendant Angela . . . would access WVU Medicine University Healthcare's patient database to obtain names, dates of birth, Social Security numbers, addresses, and driver's license numbers. . . .
>
> On or about June 27, 2016, in Berkeley County, . . . the defendants [Wayne] and [Angela] did knowingly execute such scheme and artifice . . . by accessing WVU Medicine University Healthcare's patient database and obtaining the name, date of birth, Social Security number, address, driver's license number, and a copy of [the] driver's license of the fourth person known to the Grand Jury and transferring that information to the defendant [Wayne] who then used that information to obtain a Wells Fargo Visa Signature Card with an $8,000 line of credit . . . in the name of the fourth person known to the Grand Jury[.]

That indictment is pretty clear, and it repeats the same scheme for 35 other counts for conspiracy to commit identity theft, production of false identity documents (namely Social Security cards), aggravated identity theft, and bank fraud.

[3] The record contains evidence from Wayne's plea hearing, and also contains references to Angela's meetings with her probation officer. However, the record is otherwise unclear as to what charges Angela and Wayne pleaded guilty to or were otherwise convicted of.

With that federal indictment in mind, juxtapose the criminal case with the majority opinion. On the one hand, Angela's actions were so significant, and caused so much harm to patients at WVU Hospitals, that a federal prosecutor saw fit to pursue a 36-count indictment and to use the evidence of Angela's theft of data from the hospital to support a criminal conviction. On the other hand, on the same evidence, the majority opinion concludes Angela's theft of data was "legitimate" and so insignificant that those same patients did not suffer an "injury in fact" sufficient to file a class action lawsuit for damages. This conclusion is wrong. The plaintiffs allege WVU Hospitals was careless with how it managed its patient files, failed to follow basic security procedures like conducting surveillance of its employees, and failed to encrypt information or otherwise safeguard files against wrongful activity. Angela took advantage of the hospital's carelessness. She stole patient data and gave it to a co-conspirator to commit identity theft. Something is wrong with our society when our courts say an act can support a criminal conviction beyond a reasonable doubt yet cannot support a civil claim for damages by a preponderance of the evidence.

Generally, courts rely on three factors to determine if a plaintiff sufficiently pleaded an injury-in-fact from the threat of future identity theft. The first factor hinges on the intention of the third party who gained access to the personal information. Courts are more likely to find standing where the third party had a criminal motive. The second factor looks to the type of information stolen; some information (like Social Security numbers, driver's licenses, or birthdates) is more useful for identity theft than other information. The

third factor turns on whether there is some proof the compromised, personal information was actually misused. Mitchell J. Surface, *Civil Procedure-Article III Cause-in-Fact Standing: Do Data Breach Victims Have Standing Before Compromised Data Is Misused?*, 43 Am. J. Trial Advoc. 503, 506 (2020).[4]

Applied to this case, it appears that the plaintiffs can establish an injury in fact. First, we know from Angela's deposition and the proceedings in federal court that Angela trolled through the hospital's files with the intent of stealing patient data to use in an identity-theft scheme with Wayne. Second, the information stolen – addresses, birthdates, Social Security numbers and driver's licenses – was of great use in Angela's

[4] Another journal summarized the approach taken by federal courts thusly:

> Data breach litigation has given rise to new questions, like whether claims may proceed against hacked companies in the absence of fraudulent account activity or actual identity theft affecting those whose information was lost. Courts have recognized a distinction between cases involving actual fraud or identity theft – or, at least, signs of a malicious hack – and cases not involving misuse, as where a thief may have broken into a car and grabbed a laptop without realizing what it contained. Plaintiffs in the first category, who suffered economic loss or were subject to intentional data theft, have been deemed to have standing to sue the hacked company for negligence and other alleged violations. In the second category, plaintiffs whose information was merely exposed, but never exploited, often find themselves out of luck.

Jordan Elias, *Course Correction-Data Breach As Invasion of Privacy*, 69 Baylor L. Rev. 574, 575 (2017) (emphasis added).

and Wayne's fraud scheme. And third, the compromised personal information was, in fact, misused. On this record, the plaintiffs clearly established an injury-in-fact.

The majority opinion has wrongly conflated *how* the data was stolen with whether the victims of those thefts were injured. In a run-of-the-mill data breach, financial information is stolen by an outside "hacker" who engages in fraud or identity theft. This case is different because there was no outside hacker; here, the hacker actually worked for the hospital and stole the data one file at a time. However, just because the data was stolen by someone who legitimately had access to the data does not alter the fact that the plaintiffs were injured.

In my review of how federal courts handle the injury-in-fact question, every single appellate circuit court focused on the actual impact of the theft on the victim, not whether the thief was "authorized" to commit the theft. Further, a majority of federal circuits have found an injury-in-fact exists where there is a heightened risk of identity theft subsequent to a data breach.[5] The United States Court of Appeals for the Fourth Circuit

[5] The circuits finding an injury in fact arising from a heightened risk of identity theft subsequent to a data breach include the D.C. Circuit (*In re: U.S. Office of Pers. Mgmt. Data Sec. Breach Litig*., 928 F.3d 42, 55-56 (D.C. Cir. 2019) (holding that identity theft constitutes a concrete and particularized injury because the victim is subject to a substantial risk of future fraud and identity theft); *Attias v. Carefirst, Inc*., 865 F.3d 620, 629 (D.C. Cir. 2017) ("[A] substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken."); Third Circuit (*In re Horizon Healthcare Serv. Inc. Data Breach Litig*., 846 F.3d 625, 641 (3d Cir. 2017) (noting the injury-in-fact requirement is not insurmountable, thus finding a violation of the Fair Credit Reporting Act by not protecting personal data constituted a clear de facto injury, and noting unauthorized disclosures of legally protected personal information have long been seen as injurious); *In re Nickelodeon Consumer Privacy Litig*., 827 F.3d 262, 274 (3d

has issued two cases on computer data theft demonstrating a proper analysis of the injury-in-fact question. In *Beck v. McDonald*, 848 F.3d 262, 267-76 (4th Cir. 2017), the court

---

Cir. 2016) ("The purported injury here is clearly particularized, as each plaintiff complains about the disclosure of information relating to his or her online behavior."); *In re Google Inc. Cookie Placement Consumer Privacy Litig*., 806 F.3d 125, 134-35 (3d Cir. 2015) ("Consequently, and contrary to the contentions of the defendants, a plaintiff need not show actual monetary loss for purposes of injury in fact.")); Sixth Circuit (*Galaria v. Nationwide Mut. Ins. Co*., 663 F. App'x 384, 388 (6th Cir. 2016) (finding injury-in-fact where plaintiffs' personal information was stolen but not yet misused because it is likely the information will be misused)); Seventh Circuit (*Dieffenbach v. Barnes & Noble, Inc*., 887 F.3d 826, 828 (7th Cir. 2018) (finding injury-in-fact because the victims' data was stolen and they had the opportunity to prove damages); *Lewert v. P.F. Chang's China Bistro, Inc*., 819 F.3d 963, 969 (7th Cir. 2016) (finding that some injuries plaintiffs claimed were enough to find standing); *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 696 (7th Cir. 2015) ("The injuries associated with resolving fraudulent charges and protecting oneself against future identity theft ... are sufficient to satisfy the first requirement of Article III standing.")); Ninth Circuit (*In re Zappos.com, Inc.*, 888 F.3d 1020, 1028-29 (9th Cir. 2018) (finding injury-in-fact where the plaintiffs alleged a credible threat of real and immediate harm stemming from the theft of personal information--although Social Security numbers were not included in the data breach--because there was a substantial risk the hackers would commit identity fraud or theft); *Krottner v. Starbucks Corp*., 628 F.3d 1139, 1143 (9th Cir. 2010) ("Were Plaintiffs-Appellants' allegations more conjectural or hypothetical ... we would find the threat far less credible.")); and Eleventh Circuit (*Resnick v. AvMed, Inc*., 693 F.3d 1317, 1323 (11th Cir. 2012) (finding injury-in-fact where defendants' laptops were stolen containing the plaintiffs' personal information that was misused)). *But see Whalen v. Michaels Stores, Inc*., 689 F. App'x 89, 91 (2d Cir. 2017) (finding that standing requires a future injury be certainly impending rather than simply speculative, and that because the plaintiff's personal identification information--date of birth or Social Security number--was not stolen and the plaintiff had not expended any time or effort monitoring her credit, there was no injury or threat of future injury); *In re SuperValu, Inc*., 870 F.3d 763, 768 (8th Cir. 2017) (holding plaintiffs' injury must affect the plaintiff in a personal and individual way, and that stolen credit card information that had not yet been misused is too speculative to qualify as a substantial risk of identity theft); *Katz v. Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012) (finding no injury-in-fact to satisfy the Article III standing requirement because plaintiffs' personal information was not shown to have actually been stolen, only that the defendant did not have proper security measures in place to protect the data, increasing their vulnerability to hackers and future identity fraud).

concluded a Veterans Administration hospital laptop, stolen from the backseat of a car, which contained veterans' personal information and medical records did not confer injury-in-fact standing, because the plaintiffs produced no evidence the information had been accessed or misused. Because the plaintiffs filed the lawsuit three to four years after the laptop was stolen, the court found no substantial risk that the plaintiffs were going to fall victim to identity fraud or theft. However, a year later, in *Hutton v. National Board of Examiners in Optometry, Inc*., 892 F.3d 613, 622 (4th Cir. 2018), the court distinguished *Beck* because the plaintiffs offered evidence that they had already suffered actual harm – some plaintiffs could show credit cards were fraudulently issued using stolen data – and found that the evidence supported finding the injury-in-fact requirement had been met.

Ultimately, I think the "majority rule" regarding whether a plaintiff has an injury-in-fact resulting from data theft can be distilled down to this guide found in *Khan v. Children's National Health System*, 188 F. Supp. 3d 524, 532 (D. Md. 2016):

> in the data breach context, plaintiffs have properly alleged an injury in fact arising from increased risk of identity theft if they put forth facts that provide either (1) actual examples of the use of the fruits of the data breach for identity theft, even if involving other victims; or (2) a clear indication that the data breach was for the purpose of using the plaintiffs' personal data to engage in identity fraud.

Applying the *Khan* rule to this case, the majority opinion should have found that the plaintiffs properly alleged an injury in fact arising from an increased risk of identity theft. The plaintiffs put forth evidence of actual examples where the data stolen by Angela was used to steal the identity of some of the plaintiffs. Moreover, they offered clear evidence

their files were examined and their personal data was taken for the purpose of engaging in identity fraud. Hence, all of the members of the class, including the class representatives, have properly alleged an injury in fact sufficient to permit the class action to proceed. Thus, I must conclude the majority erred in holding otherwise.

A third problem with the majority opinion is its focus on named-plaintiff Deborah Welch's "standing." The authorities cited by the majority opinion are pretty clear that "[i]n class actions, *as in all suits in federal court*, plaintiffs must have standing in order to sue." 1 William B. Rubenstein, *Newberg on Class Actions* § 2:1 (5th edition 2011) (emphasis added). The problem with the majority opinion's reasoning is that this case was filed in West Virginia state court and not in federal court. The West Virginia Constitution does not have a standing requirement like that found in Article III of the United States Constitution. As the leading treatise on class actions says, "the Article III requirements that apply to cases brought in federal court do not apply in state court." *Id.* at n.1. Hence, I would caution future courts that the majority's opinion's holding that "at least one named plaintiff must have standing with respect to each claim asserted" is built on shifting sands.

That said, the majority opinion concludes that class representative Deborah Welch does not have standing because she did not prove to the majority that she sustained a "breach" of her confidential information or an invasion of privacy caused by "an unreasonable intrusion" upon her seclusion. Syl. pt. 8, *Crump v. Beckley Newspapers, Inc.*, 173 W. Va. 699, 320 S.E.2d 70 (1983). Angela spent her first 30 seconds "legitimately accessing" Ms. Welch's file, but she spent the remainder of the time illegitimately

accessing the file. Nevertheless, the majority opinion deems Angela's entire access to the file a "reasonable" intrusion. The logical theme of the majority's opinion is that if you start to do something with good intentions, then it doesn't matter what you do later. That's akin to finding that, if a nurse walks into a room to administer medicine to a patient but then walks out of the room with an article of the patient's property, the patient would have no claim against the hospital because the nurse was "authorized" by the hospital to be in the room.

To reach its decision on standing, the majority opinion also weaves and twists to avoid the holding in *Tabata v. Charleston Area Medical Center*, 233 W. Va. 512, 759 S.E.2d 459 (2014). There, the hospital accidentally put patient data in a computer file that could be accessed from the internet. An employee was doing his or her authorized and legitimate job and just made a mistake. There was no proof anyone saw the data and no proof anyone used the data for a nefarious purpose. Still, because the patients' private data was exposed in a such a way that strangers could access it, this Court said the hospital could face liability for invading patients' privacy. In this case, the hospital opened its patient data up for employees to scroll through in a way that looked legitimate, but the employee could, at the same time, copy and use the data for an illegitimate, nefarious purpose. And did. The plaintiffs in *Tabata* had a cause of action when it was not clear anyone ever saw or illicitly used the data; here, the plaintiffs can't pursue a class action despite someone seeing the data, stealing the data, and using the data to steal patients' identities. The holdings in *Tabata* and this case cannot be reconciled.

Fourth, the majority opinion avoids discussing the variety of claims asserted in the plaintiffs' amended complaint including breach of the duty of confidentiality; unjust enrichment; negligence; breach of contract; negligent supervision; and violations of the Consumer Credit and Protection Act. The majority opinion lumps all of these claims into one and determines that all of them require proof WVU Hospitals permitted a "breach" of patients' confidential information by an outsider. Then, having declared that no breach occurred because Angela's access was "legitimate," the majority opinion finds the plaintiffs cannot support any of these causes of action. However, when we examine each of these causes of action alone, it becomes clear that the plaintiffs *can* make out a prima facie case (which, for purposes of class action status, is far more than is required). For instance, the plaintiffs allege that WVU Hospitals negligently supervised Angela.

> In a claim for negligent supervision it is the employer's wrongful act rather than the employee's wrongful act that is at issue. The focus is upon whether the employer owed a duty of care to the plaintiff and breached that duty by allowing an employee to engage in negligent, reckless, or intentional tortious conduct.

C.C. v. Harrison Cty. Bd. of Educ., 859 S.E.2d 762, 786 (W. Va. 2021) (Hutchison, J., concurring, in part, and dissenting in part) (cleaned up). The evidence of record sets out sufficient facts that a jury could say that WVU Hospitals had a duty to protect the plaintiffs' data but breached that duty by allowing Angela, as part of her job, to engage in identity theft and other tortious conduct. The fact that Angela was, in part, legitimately in every patient's file does not vitiate the fact that she eventually searched those files for data to steal, and that WVU Hospitals failed to stop her from doing so. WVU Hospitals can be

liable for negligent supervision despite the fact that Angela acted intentionally, criminally, or outside the scope of her employment. "[L]iability for negligent supervision arises when the employer permits an employee to act 'outside the scope of his employment' and causes injury to another." *Id.* at 787 (citing *Restatement (Second) of Torts* § 317 (1965)). The same analyses apply to the other causes of action in the amended complaint, and on remand the plaintiffs and circuit court should do precisely that.

Fifth, while the majority opinion finds that Ms. Welch does not have standing *to represent a class action*, the opinion fails to acknowledge that Ms. Welch still has standing to assert her individual claims. Moreover, so can the other 7,445 patients whose data was improperly accessed. *See* W. Va. Code § 55-2-18 (tolling any statute of limitation from date of an order dismissing an action). Because of the majority opinion, she, along with the thousands of other individuals, can file individual lawsuits that can be grouped together by the circuit court under West Virginia Rule of Civil Procedure 42 (allowing for consolidation of actions). WVU Hospitals can pay its lawyers to file answers to 7,445 lawsuits. And, as to damages, if the circuit court concludes the hospital's conduct was egregious, a jury can award punitive damages against WVU Hospitals for permitting Angela to view 7,445 patient files without supervision. *See Perrine v. E.I. du Pont de Nemours & Co*., 225 W. Va. 482, 553, 694 S.E.2d 815, 886 (2010) ("[I]t is within the trial court's discretion to consider other relevant aggravating and mitigating evidence" when assessing punitive damages); Syl. pt. 3, *Garnes v. Fleming Landfill, Inc*., 186 W. Va. 656,

413 S.E.2d 897 (1991) (in an award of punitive damages, juries may consider "how long the defendant continued in his actions" and "how often" similar conduct has occurred).

Sixth, I am perplexed that the majority opinion concludes that Eugene Roman is not a "typical" representative of the class. The record shows that Mr. Roman is the perfect representative because he was a direct victim of Angela and Wayne's scheme. Earlier in my dissent, I quoted from a 36-count federal indictment charging Angela and Wayne. The count that I cited, Count 33, identified "the fourth person known to the Grand Jury" whose personal information was stolen from the hospital and used to open a Wells Fargo credit card. That "fourth person" is Mr. Roman.

At Wayne's plea hearing in federal court, an FBI special agent testified that Count 33 involved Angela improperly accessing Mr. Roman's data, not once, but twice. The FBI agent testified to Angela "accessing Mr. Roman's patient profile at WVU Medicine in Berkeley County, West Virginia on June 27 and July 26, 2016," and that "Angela [did] then provide that information to [Wayne] at some point," information Wayne used to illegally apply for a Wells Fargo Credit card in Mr. Roman's name. Upon questioning by the federal judge, Wayne agreed that the FBI agent's testimony was "substantially correct" and "accurately reflect[ed]" his involvement. Stated simply, the record in this case shows Angela accessed Mr. Roman's information, delivered that information to Wayne, and he used that information to commit fraud and identity theft. Accordingly, Mr. Roman is the perfect representative for the class.

Chief Justice Walker recently said that extraordinary remedies like writs of prohibition

> are reserved for "really extraordinary causes." As we have explained, a writ of prohibition will not issue to prevent a simple abuse of discretion by a trial court. It will only issue where the trial court has no jurisdiction or having such jurisdiction exceeds its legitimate powers.

State ex rel. Vanderra Res., LLC v. Hummel, 242 W. Va. 35, 40, 829 S.E.2d 35, 40 (2019). She further found that writs of prohibition "are not available in routine circumstances." *Id.* The majority opinion in this case declares that "'[w]hether the requisites for a class action exist rests within the sound discretion of the trial court.' Syllabus Point 5, *Mitchem v. Melton,* 167 W. Va. 21, 277 S.E.2d 895 (1981)."[6] Yet, as the majority opinion demonstrates, this Court is willing to override the discretion of trial courts, in routine circumstances, to grant a writ of prohibition. I do not believe the majority opinion reflects a proper use of judicial power.

In summary, I do not believe the record or the law supports the issuance of a writ of prohibition in this case. I therefore respectfully dissent. Further, I am authorized to state that Justice Wooton joins in this dissent.

[6] ___ W.Va. at ___, ___ S.E.2d at ___ (Maj. Op. at 22).