

task of testifying, which might have required them to travel, or to take time off work. They would also be relieved from any threats that they might have faced from persons who would be adversely affected either by their testimony (e.g., the defendants, or their associates) or by its lack (e.g., the prosecutors).

A system of constant State surveillance would have other advantages, too. Under the current criminal justice system, a wealthy defendant who is innocent of the charges that she is faced with can use her wealth to hire private investigators to demonstrate her innocence, either by finding persons who witnessed the crime of which she is accused or by finding persons who can provide her with a legitimate alibi. This option is not open to poorer defendants who are similarly innocent, but who cannot afford to hire private investigators. Since this is so, innocent, poor defendants are more likely than innocent, wealthy defendants to accept plea-bargains, or to be convicted of crimes that they did not commit. If, however, a poor person were to be accused of a crime in a State that subjected its citizens to constant surveillance, the judge in her case would be morally justified (indeed, would be morally *required*) in enabling the defense to secure information that would prove her innocence, and that would have been gathered by the State's surveillance devices. A State's use of constant surveillance could thus reduce the number of persons who are wrongfully convicted. This would not only be good in itself, but it would also lead to a more equitable justice system, for the disparity in wrongful conviction rates between the wealthy, who could use their wealth to prove their innocence, and the poor could be eliminated.

In addition to these advantages constant State surveillance would also benefit the State's citizenry at large, by serving as a deterrent to crime. This would not be because the citizens who lived under State surveillance would never know when they were being watched, and so would refrain from committing crimes for fear of being caught in the act, as would persons in both 1984 and Jeremy Bentham's Panopticon.¹⁷ As is clear from the second clarification of this pro-surveillance argument, above, this argument does

not justify the State watching its citizens, for in doing so it would acquire more information about them than it is morally permitted to acquire. However, were the State to subject its citizens to the degree of surveillance that would be justified on the above argument, its citizens would know that whenever a crime was committed its performance would be recorded, and so its perpetrator would be likely to be apprehended. This knowledge would deter many potential criminals from committing crimes.¹⁸ It would also deter law enforcement officers from extending the limits of their authority.¹⁹ To be sure, the knowledge that one's criminal act would be recorded would not deter all potential criminals from committing crimes. Some persons would still commit crimes of passion, and of anger; others would succumb to the temptation to commit an opportunistic theft, act under the influence of drugs or alcohol, or act on the belief that they would not be caught. But most persons would simply judge the commission of crime not worthwhile once they realized that they were subject to constant State surveillance, and so such surveillance would serve as an effective deterrent to most criminal activity.

TWO INITIAL OBJECTIONS

Despite the advantages that would accrue to a system of constant State surveillance of the type that is defended above, there are two immediate objections that its proponents must face. The first is that such a surveillance system would be open to abuse. The second denies the claim that it is morally permissible for agents of the State (e.g., judges) to compel witness testimony or authorize information-gathering surveillance.

The Objection from Potential Abuse

The most obvious objection to a system of constant State surveillance is that it would be open to abuse. Jay Stanley and Barry Steinhardt, for example, note that the FBI's "Carnivore" program, which is "supposed to be used to tap into the email traffic of a particular individual," will filter through "all the traffic on the Internet Service Provider to which it has been attached"—and