



## PRIVACY AND CONSENT OVER TIME: THE ROLE OF AGREEMENT IN FOURTH AMENDMENT ANALYSIS

CHRISTINE JOLLS\*

Like many legal systems around the world, the American system protects the “right to privacy,” or, as Samuel Warren and Louis Brandeis famously put it, the “right to be let alone.”<sup>1</sup> Although Warren and Brandeis’s formulation has profoundly influenced privacy law, a moment of thought reveals that most of us do *not* wish to be entirely “let alone.” An individual wholly surrounded by a cocoon of solitude—for instance, the Russian mathematician who declined the equivalent of a Nobel Prize because he preferred to remain secluded in his mother’s St. Petersburg home—is a rarity (and usually at least somewhat of an oddity).<sup>2</sup> Although we do not want our homes or property to be open for inspection at all times, we usually want the police to be able to come in and take a look when we have been victims of a burglary.

Because most people want to be “let alone” in some circumstances, but not entirely, the issue of *consent* to letting another enter into one’s own sphere looms large in privacy law. As the late philosopher Joel Feinberg put it, “The root idea ... of privacy is that of a privileged territory or domain in which an individual person has the exclusive authority of determining whether another may enter, and if so, when and for how long .... Within this area, the individual person is ... boss, sovereign, owner.”<sup>3</sup> Privacy, far from referring to

---

\* Gordon Bradford Tweedy Professor of Law, Yale Law School. George Wythe Lecture, Mar. 21, 2012. I am grateful to Abbe Gluck, Neal Katyal, and Yale Law School Information Society Project workshop participants for extremely helpful comments and to Matthew Shapiro for outstanding research assistance.

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (internal quotation marks omitted).

2. See Dennis Overbye, *A Math Problem Solver Declines a \$1 Million Prize*, N.Y. TIMES, July 2, 2010, at A10.

3. 2 JOEL FEINBERG, *THE MORAL LIMITS OF THE CRIMINAL LAW* 24 (1985).

a sphere within which one is always “let alone,” refers to a sphere in which we are allowed to determine who may enter, when, and under what circumstances.

The Fourth Amendment to the United States Constitution, protecting “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,”<sup>4</sup> guards against *government* privacy invasions, and, as with other strands of privacy law, consent has long played a significant role. Under the Supreme Court’s decision in *Schneckloth v. Bustamonte*,<sup>5</sup> an individual’s voluntary agreement to a search means that no Fourth Amendment violation has occurred,<sup>6</sup> for instance, if a government official comes to my front door or to my car and asks if he or she may search my house or my car, and I say yes, then going ahead and searching my house or my car is permitted under the Fourth Amendment.<sup>7</sup> Today, “there are few areas of Fourth Amendment jurisprudence of greater practical significance than consent searches.”<sup>8</sup> Although in some cases agreement to a search might be implied from the surrounding circumstances rather than taking the express form seen in *Schneckloth*, the doctrine and analysis in this Article focus on express agreement.<sup>9</sup>

That one’s agreement is relevant—often highly so—to privacy analysis under the Fourth Amendment has been clear for decades. However, as the Fourth Amendment has confronted various features of modern life, significant fault lines around the role of agreement have appeared. The focus of this Article is some of those fault lines—and how we might go about beginning to repair them.

---

4. U.S. CONST. amend. IV.

5. 412 U.S. 218 (1973).

6. *Id.* at 219, 222-23.

7. *See, e.g., id.* at 219, 227-34.

8. 1 JOSHUA DRESSLER & ALAN C. MICHAELS, UNDERSTANDING CRIMINAL PROCEDURE § 16.01, at 247 (5th ed. 2010).

9. Often, though not always, express agreement to a search is memorialized in a written document. *See, e.g.,* Nancy Leong & Kira Suyeishi, *Consent Forms and Consent Formalism*, 2013 WIS. L. REV. (forthcoming) (manuscript at 17-30) (on file with author).

## I

Let us start with two canonical cases from the modern era.

Case 1: Imagine that a public university's employee handbook specifies that employees may be subjected to random drug testing at any time in furtherance of the university's drug-free-campus policy. Employees must sign a form their first day on the job indicating that they will submit to such drug testing. Testing is done through laboratory analysis of a urine sample, with the urine sample being produced in the presence of a monitor to preclude the possibility of adulteration of the sample.

Has every university employee "consented to" producing a urine sample in the presence of a monitor for purposes of drug testing by virtue of the provision in the employee handbook? Does a Fourth Amendment challenge therefore immediately fail on grounds of such "consent"?

Under current law, the answer is clearly "no"; courts do *not* rely on consent in resolving Fourth Amendment challenges in drug testing cases of the sort just described.<sup>10</sup> Workplace drug testing challenges under the Fourth Amendment began to rise to prominence in the late 1980s with the United States Court of Appeals for the District of Columbia Circuit's decision in *National Federation of Federal Employees v. Weinberger*.<sup>11</sup> "We hold," wrote the *Weinberger* court, "that a search otherwise unreasonable [under the Fourth Amendment] cannot be redeemed by a public employer's exaction of a 'consent' to the search as a condition of employment."<sup>12</sup>

If the Fourth Amendment outcome is not determined by consent in a case such as *Weinberger*, then how is that outcome determined? Courts in such cases engage in a substantive balancing of two general interests: the employee's privacy interest in not performing "an excretory function traditionally shielded by great privacy"<sup>13</sup> at the request of, and with monitoring by, the employee's public employer; and the public employer's interest in detecting and deterring illegal

---

10. See sources cited *infra* notes 11, 16.

11. 818 F.2d 935 (D.C. Cir. 1987).

12. *Id.* at 943.

13. *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 626 (1989).

drug use in service of “the efficient and proper operation of the workplace.”<sup>14</sup> The question of whether workplace drug testing violates the Fourth Amendment turns on the relative weight of these two interests. Although “[a]dvance notice” of the workplace drug testing “may be taken into account as one of the factors relevant to the extent of the employees’ legitimate expectations of privacy” (the first interest),<sup>15</sup> the legal framework remains one of balancing of the two substantive interests rather than a simple on-off switch of “consent.”

The *Weinberger* court’s adoption of a substantive balancing test in lieu of a consent-based approach to workplace drug testing is reflected in other circuits’ case law as well.<sup>16</sup> An opinion written by Judge Wilkinson of the United States Court of Appeals for the Fourth Circuit in 2000 is illustrative. Notwithstanding an employee’s signed drug testing agreement from his first day on the job, Judge Wilkinson’s analysis of the employee’s subsequent challenge to workplace drug testing focused *not* on the “consent” of the employee but rather on the importance of the government employer’s interests in drug testing in relation to the employee’s privacy interests.<sup>17</sup> “[T]he permissibility of a particular [search] is judged by balancing its intrusion on the individual’s Fourth Amendment interests against its promotion of legitimate governmental interests.”<sup>18</sup> Judge Wilkinson proceeded to analyze the challenged workplace drug testing on the basis of the strength of those interests—not based on any notion of the employee’s “consent.”<sup>19</sup>

Consider now a second paradigmatic case of our era, involving workplace computer surveillance.

Case 2: Materials gathered by a professor at a public university for a book he is writing include hundreds of controversial images, which he has stored on his computer hard drive. The university faculty manual provides that university computers may be moni-

---

14. *Weinberger*, 818 F.2d at 942 (quoting *O’Connor v. Ortega*, 480 U.S. 709, 723 (1987)).

15. *Id.* at 943.

16. *See, e.g.*, *Carroll v. City of Westminster*, 233 F.3d 208, 211 (4th Cir. 2000); *Aubrey v. Sch. Bd. of Lafayette Parish*, 148 F.3d 559, 562 (5th Cir. 1998); *McDonell v. Hunter*, 809 F.2d 1302, 1307-08 (8th Cir. 1987).

17. *Carroll*, 233 F.3d at 211.

18. *Id.* (quoting *Skinner*, 489 U.S. at 619).

19. *Id.*

tored or scanned at any time. The professor signed a form the first day on the job acknowledging receipt of the manual and the professor's acceptance of its provisions. Nine years later, the professor learns that his hard drive, with its controversial material, has recently been comprehensively imaged by the university computer services department. Did the professor, in signing the form presented to him on his first day on the job, "consent" to the comprehensive imaging, such that the imaging is automatically permissible under the Fourth Amendment?

In today's Fourth Amendment case law on computer surveillance, we see some courts adopting the type of consent argument that was squarely rejected in the drug testing context discussed above. Interestingly, the most prominent of the rulings adopting consent analysis in the context of computer surveillance was decided by the United States Court of Appeals for the Fourth Circuit within a few months of the Judge Wilkinson opinion discussed above.

The Fourth Circuit surveillance case, *United States v. Simons*,<sup>20</sup> arose from the imaging of an employee's hard drive after the employee had come under suspicion of harboring child pornography on his computer.<sup>21</sup> The Fourth Circuit panel, not including Judge Wilkinson, dismissed the employee's Fourth Amendment challenge to the computer surveillance on the ground that the employee did not "assert that he was unaware of, or that he had not consented to, the [workplace] Internet policy," which allowed the employer to "inspect, and/or monitor the user's [computer]."<sup>22</sup> The court held that in light of the employee's "consent," there was no need to engage in any balancing of his privacy interests versus the government's interests in workplace efficiency and safety.<sup>23</sup> Because of the employee's "consent," the Fourth Amendment argument seemed to be over before it even really began.

In the years following *Simons*, several other cases have taken a similar approach to computer surveillance. In *United States v. Thorn*,<sup>24</sup> for instance, the United States Court of Appeals for the

---

20. 206 F.3d 392 (4th Cir. 2000).

21. *Id.* at 396.

22. *Id.* at 396, 398 n.8.

23. *Id.* at 398 & n.8.

24. 375 F.3d 679 (8th Cir. 2004), *vacated on other grounds*, 543 U.S. 1112 (2005).

Eighth Circuit ruled against a government employee's challenge to workplace computer surveillance on the ground that the employee "was fully aware of the computer-use policy, as evidenced by his written acknowledgement of the limits imposed on his computer-access rights," including the provision that he had "no personal right of privacy with respect to" his employer's computers.<sup>25</sup> Likewise, the court in *United States v. Gavegnano*<sup>26</sup> rejected a child pornography defendant's Fourth Amendment challenge to computer surveillance on the ground that when he "was issued a government computer, the user agreement he signed stated that he was aware of the acceptable use of all government-issued information systems, [and] that he consented to the monitoring of the information systems."<sup>27</sup>

The approach to computer surveillance adopted in *Simons* has not been universally followed. For example, a 2007 opinion by the United States Court of Appeals for the Ninth Circuit following a petition for rehearing of a 2006 case suggested an appreciation for the far-reaching implications of *Simons's* divergence from the approach in the drug testing cases discussed above.<sup>28</sup> The 2007 opinion withdrew the earlier opinion—an opinion that had unreservedly applied *Simons*:

Upon their hiring, [the company's] employees were apprised of the company's monitoring efforts through training and an employment manual, and they were told that the computers were company-owned and not to be used for activities of a personal nature.... Like *Simons*, [the employee here] "does not assert that he was unaware of, or that he had not consented to, the Internet [and computer] policy."<sup>29</sup>

In the 2007 opinion, the Ninth Circuit, unequivocally eschewing any reliance on this reasoning, instead emphasized the importance of Ziegler's privacy rights in the *office* within which the computer was located:

---

25. *Id.* at 683.

26. 305 F. App'x 954 (4th Cir. 2009) (per curiam).

27. *Id.* at 955-56.

28. *United States v. Ziegler*, 474 F.3d 1184 (9th Cir. 2007).

29. *United States v. Ziegler*, 456 F.3d 1138, 1144 (9th Cir. 2006) (last alteration in original) (quoting *United States v. Simons*, 206 F.3d 392, 398 n.8 (4th Cir. 2000)), *withdrawn by Ziegler*, 474 F.3d 1184.

Ziegler's expectation of privacy in his office was reasonable on the facts of this case....

Had the company computer assigned to Ziegler ... been physically located outside a private office, we might have had to consider whether Ziegler had a reasonable expectation of privacy in the device itself, in the face of a corporate policy of monitoring the corporate computers. However, we leave that question for another day.<sup>30</sup>

To be sure, the facts giving rise to Ziegler's Fourth Amendment challenge provided, in the court's view, an alternative ground on which to rule against this challenge.<sup>31</sup> Unlike Simons, Ziegler was not a government employee, and thus the search was conducted not by the government in its role as employer, but instead by the government in its law enforcement capacity in cooperation with Frontline Processing, Ziegler's private employer.<sup>32</sup> In these circumstances, wrote the court in the 2007 opinion, "the government ... may show that permission was obtained from a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected."<sup>33</sup> In concluding that Frontline "exercised common authority over the office and the workplace computer such that it could validly" permit the government's search, the court relied on several factors, including Frontline's pervasive control over Ziegler's company-owned computer and the fact that employees "were apprised of the company's monitoring" of such computers<sup>34</sup>—just as the *Weinberger* court concluded that advance notice of workplace drug testing could be "taken into account as one of the factors relevant to the extent of the employees' legitimate expectations of privacy."<sup>35</sup> Still, the Ninth Circuit clearly

---

30. *Ziegler*, 474 F.3d at 1190 & n.9 (internal citation omitted).

31. *See id.* at 1191-92.

32. *Id.* Several judges dissented from the denial of en banc review of the 2007 opinion on the ground that, in these judges' view, no valid agreement to the search by Ziegler's employer existed. *See United States v. Ziegler*, 497 F.3d 890, 895-99 (9th Cir. 2007) (W. Fletcher, J., dissenting from the denial of en banc review); *id.* at 900-01 (Kozinski, J., dissenting from the denial of en banc review).

33. *Ziegler*, 474 F.3d at 1191 (internal quotation marks omitted).

34. *Id.* at 1191-92.

35. *Nat'l Fed'n of Fed. Emps. v. Weinberger*, 818 F.2d 935, 943 (D.C. Cir. 1987).

stepped back from the *Simons*-based consent analysis offered in the opinion the court chose to withdraw.<sup>36</sup>

---

36. See *Ziegler*, 474 F.3d at 1185 (withdrawing previous opinion); *supra* text accompanying note 30 (court's reservation of question addressed in *Simons*).

In the view of one of two Ninth Circuit opinions dissenting from the denial of en banc review of the new ruling in *Ziegler*, "the only analysis provided to substantiate Frontline's authority to consent [was] a description of Frontline's computer monitoring policy." *Ziegler*, 497 F.3d at 896 (W. Fletcher, J., dissenting from the denial of en banc review) (citing *Ziegler*, 474 F.3d at 1191-92). However, the new ruling's analysis of Frontline's authority to consent in fact seemed to rest heavily, although not exclusively, on Frontline's ownership rights in *Ziegler*'s workplace computer and various other factors suggesting Frontline's "mutual access and joint use," *id.* at 896, of the computer:

Frontline could give valid consent to a search of the contents of the hard drive of *Ziegler*'s workplace computer because the computer is the type of workplace property that remains within the control of the employer "even if the employee has placed personal items in [it]." In [*O'Connor v. Ortega*, the Supreme Court offered an analogy that is helpful to our resolution of this question. The Court posited a situation where an employee brings a piece of personal luggage to work and places it within his office. The Court noted that "[w]hile ... [whatever expectation of privacy the employee has in] the outward appearance of the luggage is affected by its presence in the workplace, the employee's expectation of privacy in the contents of the luggage is not affected in the same way." The Court further explained that "[t]he appropriate standard for a workplace search does not necessarily apply to a piece of closed personal luggage, a handbag or a briefcase that happens to be within the employer's business address."

The workplace computer, however, is quite different from the piece of personal luggage which the Court described in *Ortega*. Although use of each Frontline computer was subject to an individual log-in, ... IT-department employees "had complete administrative access to anybody's machine." The company had also installed a firewall, which ... is "a program that monitors Internet traffic ... from within the organization to make sure nobody is visiting any sites that might be unprofessional." Monitoring was routine, and the IT department reviewed the log created by the firewall "[o]n a regular basis," sometimes daily if Internet traffic was high enough to warrant it. Finally, upon their hiring, Frontline employees were apprised of the company's monitoring efforts through training and an employment manual, and they were told that the computers were company-owned and not to be used for activities of a personal nature.

In this context, *Ziegler* could not reasonably have expected that the computer was his personal property, free from any type of control by his employer. The contents of his hard drive ... were work-related items that contained business information and which were provided to, or created by, the employee in the context of the business relationship. *Ziegler*'s downloading of personal items to the computer did not destroy the employer's common authority. Thus, Frontline, as the employer, could consent to a search of the office and the computer that it provided to *Ziegler* for his work.

*Ziegler*, 474 F.3d at 1191-92 (first, third, fifth, and sixth alterations in original) (internal citations and emphasis omitted). This treatment of Frontline's authority to consent seems to suggest that the company's ownership of *Ziegler*'s workplace computer and much of its content—and not merely the company's "computer monitoring policy," *Ziegler*, 497 F.3d at 896



## II

Viewed against the backdrop of the conventional role of consent in Fourth Amendment doctrine, the workplace drug testing cases discussed in Part I initially seem to present something of a puzzle. In general, when an individual voluntarily agrees to a search, the search is, for that reason, permissible under the Fourth Amendment.<sup>37</sup> Why, then, is a substantive balancing of interests needed in cases in which employees agree at the time of hiring that they will submit to drug testing at any point over the course of their term of employment?

One obvious answer is that agreement in such a case is not “voluntary”; employees may well suffer dire consequences if they fail to agree.<sup>38</sup> Without in any way disputing the force of that argument, this Part offers an additional, less familiar way to understand the legal treatment of the sort of agreement discussed in the workplace drug testing cases in Part I—a way that turns out to yield certain distinctive implications, as discussed more fully in Part IV below.

When an individual agrees to a law enforcement officer’s request to search, agreement is typically virtually *contemporaneous with the search itself*: there has been a knock on the door, someone is standing there when I open the door, I give that person my permission to search, and the search happens. I am not asked to give my general agreement to searches that might or might not occur at undetermined points in the perhaps-distant future. The workplace drug testing context is quite different. At the time a drug testing agreement is signed, drug testing is often not imminent, and in fact the odds that a given employee will ever be tested may be quite small; drug testing—especially accurate drug testing—is expensive,

---

(W. Fletcher, J., dissenting from the denial of en banc review)—produced the conclusion that Frontline had authority to consent to the government’s search.

37. See, e.g., *Schneckloth v. Bustamonte*, 412 U.S. 218, 222-23 (1973).

38. Cf. Legal Issues Relating to the Testing, Use & Deployment of an Intrusion-Detection Sys. (EINSTEIN 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. 1 (2009) [hereinafter *Einstein*], available at <http://www.justice.gov/olc/2009/e2-issues.pdf>, at \*15 (“In the context of public employment, ... merely obtaining the consent of an employee to search is not necessarily coextensive with the requirements of the Fourth Amendment. Such consent must be voluntary and cannot be obtained through duress or coercion.”).

and in many workplaces it dampens employee morale and loyalty as well.

The *uncertainty* in the second case, in contrast to the imminence and certainty in the first case, is extremely important. It is much easier to be confident in human judgment when the decision maker is at the threshold of a decision—the situation is about to unfold, right then and there, for sure—than it is to be confident in human judgment when the decision maker confronts a hypothetical possibility that might or might not occur down the road. The central task of this Part will be to describe the basis for this distinction. Once the importance of the distinction is appreciated, the gap between the *Simons* approach—giving controlling force to in-advance agreement—and mainstream doctrine under the Fourth Amendment comes into focus.

For it is not only in the workplace drug testing context that courts adjudicating Fourth Amendment challenges to government searches have declined to draw an inference of consent from an in-advance agreement. The Supreme Court pointedly avoided making such an inference in *United States v. Knights*,<sup>39</sup> which involved a Fourth Amendment challenge to a probation agreement specifying that the probationer could be searched “at anytime, with or without a search warrant, warrant of arrest or reasonable cause” throughout the term of his probation.<sup>40</sup> The Court, in an opinion by Chief Justice Rehnquist, declined to address the question on which certiorari had been granted in the case: whether “agreement to a term of probation that authorized any law enforcement officer to search [the parolee’s] person or premises with or without a warrant, and with or without individualized suspicion of wrongdoing, constituted a valid consent.”<sup>41</sup> “We need not decide,” the Chief Justice wrote, “whether *Knights*’ acceptance of the search condition constituted consent in the *Schneckloth* sense of a complete waiver of his Fourth Amendment rights, however, because we conclude that the search of *Knights* was reasonable”—reasonableness being the “touchstone of the Fourth Amendment.”<sup>42</sup> The reasonableness analysis, the Court continued, requires “assessing, on the one hand, the degree

---

39. 534 U.S. 112 (2001).

40. *Id.* at 114.

41. Brief for the United States at I, *Knights*, 534 U.S. 112 (No. 00-1260).

42. *Knights*, 534 U.S. at 118.

to which [a search] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."<sup>43</sup> In this analysis, the probation agreement was one "salient circumstance"<sup>44</sup>—much as the forms of advance notice in *Weinberger* and *Ziegler* factored into the multi-pronged Fourth Amendment analyses undertaken in those cases.<sup>45</sup> Thus, despite the Department of Justice's insistent contention in its brief in *Knights* that an individual may "give valid and binding prospective consent to a category of searches to be performed at unspecified times in the future,"<sup>46</sup> the Court—in the hands of a jurist renowned for his deference to law enforcement views<sup>47</sup>—refused the government's invitation to adopt a *Simons*-type consent analysis.<sup>48</sup>

43. *Id.* at 118-19 (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)).

44. *Id.* at 118.

45. See *supra* notes 34-35 and accompanying text.

46. Brief for the United States, *supra* note 41, at 8.

47. See, e.g., R. Ted Cruz, *In Memoriam: William H. Rehnquist*, 119 HARV. L. REV. 10, 10 (2005).

48. *Knights*, 534 U.S. at 118. In the earlier case of *Zap v. United States*, the Court appeared to give heavy weight to the fact that the defendant had agreed as a condition of receiving a military contract from the government to permit inspection and audit at all times of the corporate books at the defendant's place of business. 328 U.S. 624, 627-28 (1946), *vacated on other grounds*, 330 U.S. 800 (1947). The Department of Justice's brief in *Knights* relied prominently on *Zap*:

*Zap* further establishes the proposition—central to this case—that a consent to search may be granted in advance, and without specific restrictions. The defendant in *Zap* did not give consent at the time the search was conducted; to the contrary, he attempted (unsuccessfully) to prevent the search from occurring. 328 U.S. at 627. The Court nevertheless found that the defendant was bound by his prior contractual commitment to permit inspection of his books and records. *Zap* makes clear that an individual may give valid and binding prospective consent to a *category* of searches to be performed at unspecified times in the future.

Brief for the United States, *supra* note 41, at 16-17. The Court's eschewal of this reasoning in *Knights* may suggest that something about the military contracting context, rather than a general inference of Fourth Amendment consent from in-advance agreement, produced the result in *Zap*.

Prior to *Knights*, the Supreme Court decided a major Fourth Amendment case involving drug testing in the government workplace, see *Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656 (1989), but that case did not involve the sort of in-advance agreement discussed in Part I because agreement to the drug testing in *Von Raab* was required only at the time of transfer or promotion to specifically designated positions. *Id.* at 659, 663-64. Other Supreme Court drug testing cases under the Fourth Amendment have involved such contexts as drug testing of student-athletes, see *Vernonia Sch. Dist. v. Acton*, 515 U.S. 646 (1995), and government regulation requiring drug testing by private employers, see *Skinner v. Ry. Labor Excs.' Ass'n*, 489 U.S. 602 (1989).

Granting dispositive weight to in-advance agreement, as in *Simons*, departs not only from mainstream Fourth Amendment doctrine but also from common law privacy doctrine. Under a long line of common law cases, actions that “unreasonably intrude” on the “seclusion” of another person are tortious even if the person has given in-advance agreement to the actions, although they are *not* tortious if the person has given contemporaneous agreement to them.<sup>49</sup> For instance, intrusion upon seclusion challenges to private-sector workplace drug testing purportedly authorized by an in-advance agreement are routinely resolved on the basis of substantive balancing of employees’ and employers’ interests (just as under the Fourth Amendment)—*not* on the basis of the in-advance agreement.<sup>50</sup> Similarly, intrusion upon seclusion cases addressing workplace computer surveillance either entirely eschew reliance on in-advance computer monitoring policies<sup>51</sup> or, at a minimum, avoid the sort of blanket consent-based reasoning found in *Simons*.<sup>52</sup> Long-standing common law precedent thus supports the approach to in-advance agreement described in Part I’s discussion of Fourth Amendment challenges to workplace drug testing—and is at odds with *Simons*’s approach to in-advance agreement to surveillance of workplace computers.

Might it be sensible to have greater confidence in human judgment when decision makers provide their contemporaneous agreement than when they enter into an in-advance agreement governing uncertain future behavior? A couple of interesting reasons support such a distinction, but this Part focuses on one particularly important factor. Richard Thaler, a behavioral economist at the University of Chicago, likes to offer the following account of typical thinking about a future uncertain event or outcome:

Before the start of Thaler’s class in Managerial Decision Making, students fill out an anonymous survey on the course

---

49. See Christine Jolls, Privacy, Consent, and Time 9-31 (unpublished manuscript) (on file with author).

50. See, e.g., *Hennessey v. Coastal Eagle Point Oil Co.*, 609 A.2d 11, 13, 19-24 (N.J. 1992).

51. See *Garrity v. John Hancock*, No. CIV.A. 00-12143-RWZ, 2002 WL 974676, at \*1-2 (D. Mass. May 7, 2002).

52. See Jolls, *supra* note 49, at 33-34, 37 (discussing *Kelleher v. City of Reading*, No. CIV.A.01-3386, 2002 WL 1067442 (E.D. Pa. May 29, 2002), and *Thygeson v. U.S. Bancorp*, No. CV-03-467-ST, 2004 WL 2066746 (D. Or. Sept. 15, 2004) (magistrate judge opinion)).

Web site. One of the questions is “In which decile do you expect to fall in the distribution of grades in this class?” Students can check the top 10 percent, the second 10 percent, and so forth. Since these are MBA students, they are presumably well aware that in any distribution, half the population will be in the top 50 percent .... And only 10 percent of the class can, in fact, end up in the top decile.

...[T]he results of this survey reveal a high degree of unrealistic optimism .... Typically less than 5 percent of the class expects their performance to be [in the bottom 50 percent] and more than half the class expects to perform in [the top 20 percent].<sup>53</sup>

The same phenomenon turns out to apply to professors: about “94 percent of professors at a large university were found to believe that they are better than the average professor.”<sup>54</sup>

Just like most of the MBA students in Thaler’s class think they will score much higher than average (even though, by brute definition, the majority of the class cannot be above average), many people confronting other types of uncertain life events tend to assume that “it will be fine,” that it will be someone else who gets divorced, fails to be promoted, dents another car in the parking garage, or gets caught in a drug testing net at work.<sup>55</sup> By contrast, when someone is standing right in front of me and asks for my agreement to a search of my house or my car, I cannot help but realize that if I say yes, the search *will* happen. That critical rationality-encouraging feature of certainty (and the immediacy that is virtually a necessary condition for certainty) is absent when agreement is sought to something that may or may not arise at some point down the road.

The account of in-advance versus contemporaneous agreement offered here implies that eschewing consent in cases of in-advance agreement, as in the workplace drug testing cases discussed in Part I, has much to recommend it. The contrary *Simons* approach departs from mainstream Fourth Amendment doctrine, from long-

---

53. RICHARD H. THALER & CASS R. SUNSTEIN, *NUDGE* 31-32 (2008).

54. *Id.* at 32.

55. Recent economics literature identifies a rigorous framework for identifying optimistically biased perceptions in a population. See Jean-Pierre Benoit & Juan Dubra, *Apparent Overconfidence*, 79 *ECONOMETRICA* 1591 (2011); Christoph Merkle & Martin Weber, *True Overconfidence: The Inability of Rational Information Processing to Account for Apparent Overconfidence*, 116 *ORGANIZATIONAL BEHAV. & HUM. DECISION PROCESSES* 262 (2011).

standing common law privacy case law, and from behavioral economics analysis of in-advance versus contemporaneous agreement.

Of course, the reduced reliability of human judgment in an in-advance agreement as opposed to a contemporaneous agreement may not be the only important factor in determining the proper legal treatment of an in-advance agreement under the Fourth Amendment. In the *Knights* context of probation agreements, for instance, the government contended that criminal defendants could be significantly harmed by the failure to credit in-advance search agreements because “trial judges might be less willing to offer probation if they lacked assurance that the probationer’s compliance with the conditions of release could be closely monitored.”<sup>56</sup> If, in a given context, the failure to credit in-advance agreements ran a serious risk of greatly undercutting an entire category of transactions (such as the granting of probation), then, despite the limits on human judgment often associated with in-advance agreements, crediting such agreements might make a good deal of sense. The suggestion here is not that in-advance agreements are fatally compromised in every conceivable context, just that the argument for giving them effect in a case such as *Simons* is not to be found in existing Supreme Court or common law doctrine and must rely on factors weighty enough to overcome the limits on human judgment typically associated with such agreements.

### III

Despite the departure of the *Simons* approach from the precedent and analysis described above, the Department of Justice has aggressively deployed *Simons* in important controversies in recent years. Both in a lengthy 2009 memorandum on computer surveillance of United States government employees and in Supreme Court briefing the following year, the Department of Justice treated in-advance agreement and contemporaneous agreement as entirely interchangeable for Fourth Amendment purposes.

---

56. Brief for the United States, *supra* note 41, at 8.

*The Department of Justice's "EINSTEIN" Memorandum*

EINSTEIN is a United States computer surveillance system designed to protect government network traffic from malicious activity.<sup>57</sup> EINSTEIN 1.0, which originated in 2004, involved monitoring "packet header" material such as the information packet's source and destination Internet Protocol (IP) addresses and the date and time of packet transmission.<sup>58</sup> No examination of the content of packets occurred under EINSTEIN 1.0.<sup>59</sup>

EINSTEIN 2.0, launched in 2008, added surveillance of content information and, accordingly, raised Fourth Amendment issues that were not in play with EINSTEIN 1.0.<sup>60</sup> Courts have consistently held that noncontent information associated with communications technologies—information such as phone numbers dialed, IP addresses used, and date and time of the communication—does not receive Fourth Amendment protection;<sup>61</sup> by contrast, content information has traditionally received a high level of Fourth Amendment protection.<sup>62</sup>

The year after EINSTEIN 2.0's launch, the Department of Justice released a lengthy memorandum analyzing the new computer surveillance system under the Fourth Amendment.<sup>63</sup> At the heart of the Department of Justice's reasoning about the status of EINSTEIN 2.0 was the assertion, repeatedly invoked in the Department of Justice memorandum, that *either* a daily log-on banner requiring an employee's agreement in order to sign in each work day *or* a general in-advance computer-use agreement of the sort in the *Simons* case rendered EINSTEIN 2.0 permissible, on grounds of "consent," under the Fourth Amendment.<sup>64</sup> The Department's memorandum relied

---

57. Einstein, *supra* note 38, at \*2-3.

58. *Id.* at \*2; U.S. DEP'T OF HOMELAND SEC., PRIVACY COMPLIANCE REVIEW OF THE EINSTEIN PROGRAM 2 (2012), available at [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_privcomrev\\_nppd\\_ein.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_privcomrev_nppd_ein.pdf).

59. Einstein, *supra* note 38, at \*2.

60. *Id.* at \*7-8; U.S. DEP'T OF HOMELAND SEC., *supra* note 58, at \*2.

61. See, e.g., *Smith v. Maryland*, 442 U.S. 735, 741-45 (1979) (phone numbers); *United States v. Forrester*, 512 F.3d 500, 504, 510-11 (9th Cir. 2008) ("packet header" material).

62. See, e.g., *Katz v. United States*, 389 U.S. 347, 351-59 (1967) (content of telephone conversation); *United States v. Warshak*, 631 F.3d 266, 284-86, 288 (6th Cir. 2010) (content of e-mail messages).

63. See Einstein, *supra* note 38.

64. See, e.g., *id.* at \*15 ("An Executive Branch employee who clicks 'I agree' in response to the model log-on banner, enabling him to use Government-owned information systems to

specifically on *Simons*—as well as on another case discussed in Part I above, *United States v. Thorn*.<sup>65</sup>

---

access the Internet, or an employee who signs the model computer-user agreement, thereby acknowledging his 'consent[.]' to monitoring of his use of those systems, certainly appears to have consented expressly to the scanning of his incoming and outgoing Internet communications." (alteration in original) (emphasis added)); see also *id.* at \*1 ("An intrusion-detection system known as EINSTEIN 2.0 used to protect civilian unclassified networks in the Executive Branch against malicious network activity complies with the Fourth Amendment ... provided that certain log-on banners or computer-user agreements are consistently adopted, implemented, and enforced by executive departments and agencies using the system."); *id.* ("[A]s long as [entities] ... participating in EINSTEIN 2.0 operations consistently adopt, implement, and enforce the model log-on banner or computer-user agreement—or log-on banners or computer-user agreements with terms that are substantially equivalent to those models—the use of EINSTEIN 2.0 technology to detect computer network intrusions and exploitations against Federal Systems complies with the Fourth Amendment."); *id.* at \*6 ("[T]he deployment, testing, and use of EINSTEIN 2.0 technology complies with the Fourth Amendment where each EINSTEIN 2.0 Participant consistently adopts and implements the model log-on banner or model computer-user agreement—or a log-on banner or computer-user agreement containing substantially equivalent terms."); *id.* at \*9 ("[W]e believe that an ... employee will not have a legitimate expectation of privacy in the content of his Internet communications transmitted over Government-owned information systems, provided that EINSTEIN 2.0 Participants consistently adopt, implement, and enforce appropriate consent and notification procedures, such as the model log-on banner or model computer-user agreement."); *id.* at \*11 ("[W]e believe that an ... employee who has clicked through the model log-on banner or signed the model computer-user agreement ... would not have a legitimate expectation of privacy in the contents of Internet communications made using Government-owned information systems and transmitted over Federal Systems."); *id.* at \*21 ("[W]e ... conclude that an Executive Branch employee's agreement to the terms of the model log-on banner or the model computer-user agreement, or those of a banner or user agreement that are substantially equivalent to those models, constitutes valid, voluntary consent to the reasonable scope of EINSTEIN 2.0 operations.").

Although the Department of Justice's preferred line of argument appears to be based on "consent," its memorandum suggests in the alternative that a daily log-on banner or in-advance computer-use agreement renders computer surveillance with EINSTEIN 2.0 "reasonable" under the Fourth Amendment. See, e.g., *id.* at \*18 ("[R]easonableness analysis requires balancing the 'invasion of the employees' legitimate expectation of privacy against the government's need for supervision, control, and the efficient operation of the workplace.' ... [See *United States v. Knights*], 534 U.S. [112,] 118-19 [(2001)] (reasonableness inquiry balances, 'on the one hand, the degree to which [a search] intrudes upon an individual's privacy and, on the other, the degree to which a search is needed for the promotion of legitimate governmental interests') .... Based upon the information available to us, we believe that EINSTEIN 2.0 operations are reasonable under the totality of the circumstances.").

65. See 375 F.3d 679 (8th Cir. 2004), *vacated on other grounds*, 543 U.S. 1112 (2005); *Einstein*, *supra* note 38, at \*10 ("[T]he federal courts of appeals have held that the use of log-on banners or computer-user agreements ... can eliminate any legitimate expectation of privacy in the content of Internet communications made at work using Government-owned information systems. For example, in *United States v. Simons*, the computer-use policy ... expressly noted that [the employer] would audit, inspect, and/or monitor employees' use of the Internet, including all file transfers, all websites visited and all e-mail messages, as deemed



The discussion in Part II, however, suggests that the daily log-on agreement and the in-advance computer-use agreement should not be treated in this sort of undifferentiated fashion. An individual who affirmatively agrees each day, upon signing in, to a prominent, clear statement about computer monitoring undertaken by the employer will not typically face the type of uncertainty that Part II suggested may underlie *Weinberger's* and other cases' eschewing of consent reasoning under the Fourth Amendment. At the Department of Justice itself, signing in to one's computer requires one to give express agreement to a daily log-on banner containing the following language (which is used in the Department of Justice's memorandum to illustrate acceptable log-on banner language):

By using this information system, you understand *and consent* to the following:

- You have no reasonable expectation of privacy regarding any communications transmitted through or data stored on this information system.
- At any time, the Government may monitor, intercept, search and/or seize data transiting or stored on this information system.
- Any communications transmitted through or data stored on this information system may be disclosed or used for any U.S. Government-authorized purpose.

[click button: I AGREE]<sup>66</sup>

---

appropriate. The Fourth Circuit held that this policy placed employees on notice that they could not reasonably expect that their Internet activity would be private .... The Eighth Circuit came to the same conclusion in *United States v. Thorn*. In *Thorn*, a state employee had acknowledged in writing a computer-use policy, which warned that employees do not have any personal privacy rights regarding their use of [the agency's] information systems and technology.... As a result of this policy, the court held that the state employee did not have any legitimate expectation of privacy with respect to the use and contents of his [work] computer, because under the agency's policy, employees have no personal right of privacy with respect to their use of the agency's computers." (third and fourth alterations in original) (internal quotation marks and citations omitted)); *id.* at \*11 ("[T]he model log-on banner and computer-user agreement [discussed in *Einstein*] ... are at least as robust as—and we think they are even stronger than—the materials that eliminated an employee's legitimate expectation of privacy in the content of Internet communications in *Simons* [and] *Thorn*.").

66. *Einstein*, *supra* note 38, at \*6 n.5 (emphasis added).

Consent via one-time, in-advance agreement to a general computer-use policy authorizing whatever type of computer surveillance an employer might, at some point in the future, choose to undertake (or not undertake), however, differs from the contemporaneous and definite form of agreement associated with a daily log-on banner. (To be sure, a widely publicized employer practice of *not* engaging in the monitoring specified by a daily log-on banner could start to undercut the distinction drawn here between a daily log-on banner and a general in-advance computer-use policy—a point to which Part IV returns.) The Department of Justice’s discussion in its EINSTEIN memorandum would cohere far better with the precedent and analysis discussed in this Article if the discussion differentiated between contemporaneous agreement to specific forms of computer surveillance presently in use, on the one hand, and in-advance agreement to unspecified and indefinite future monitoring, on the other.

The very fact that daily log-on banners are so easily available to employers in a practical sense underlines how little is lost, from the perspective of the government’s interests, in rejecting the approach taken in the *Simons* case. The same conclusion holds true with respect to surveillance of pagers—the subject of the Supreme Court’s 2010 decision in *City of Ontario v. Quon*.<sup>67</sup>

### *The Department of Justice’s Quon Brief*

The dispute in *Quon* arose from a government employer’s review of communications sent over text-messaging pagers the employer had issued to its employees.<sup>68</sup> In arguing that the employees could have no “reasonable expectation of privacy” in communications sent over the pagers—a position that was not adopted by the Supreme Court in its eventual decision<sup>69</sup>—the Department of Justice’s brief in *Quon* toggled back and forth between the daily log-on banners used by, among others, the Department itself and the highly general “catch-all” computer-use policy used by the employer in *Quon*.<sup>70</sup> As

---

67. 130 S. Ct. 2619 (2010).

68. *Id.* at 2624.

69. *Id.* at 2629-30.

70. See Brief for the United States at 9, 11-13, 21, *Quon*, 130 S. Ct. 2619 (No. 08-1332) (“reasonable expectation of privacy” test); *infra* note 72 and accompanying text (discussion of

in its EINSTEIN 2.0 Memorandum, the Department of Justice suggested in its *Quon* brief—wrongly in the view of this Article—that in-advance and contemporaneous agreement may be treated in an aggregate fashion.

The Department of Justice's argument in its *Quon* brief began with the general principle that "[w]hen a government employer gives its employee access to a device or facility, but explicitly reserves its own right of access, the employee has no reasonable expectation of a right" against employer surveillance of that device or facility.<sup>71</sup> Following the opening section featuring this statement, the brief, in the next stage of the Department of Justice's argument, referred in immediate succession to the *Simons* case and its progeny (including the *Thorn* case noted above) and to "electronic banner[s] or splash screen[s] that warn[] the user each time he log[s] on to the computer system that his computer use [i]s subject to monitoring."<sup>72</sup> This fusing of the two distinct forms of agreement is especially striking on the specific facts in *Quon* because the written computer-use policy in the case did not so much as mention pagers, which were not yet in use among members of the employer's staff when the policy was formulated.<sup>73</sup> The computer-use policy by its terms simply reserved the employer's right "to monitor and log all network activity including e-mail and Internet use";<sup>74</sup> the employer's argument that pagers were covered was based on statements by the individual charged with administering the pagers that messages sent on the pagers were "considered e-mail messages" and, thus, were subject to monitoring.<sup>75</sup> Unquestionably, a daily "pager banner" would have done much more than a general policy that in its formal statement did not even mention pagers to generate a reliable inference of lack of a reasonable expectation of privacy on the part of the employees in *Quon*.<sup>76</sup>

---

log-on banners and general computer-use policies in Brief for the United States).

71. Brief for the United States, *supra* note 70, at 12.

72. *Id.* at 16-17 (internal quotation marks omitted).

73. *Quon*, 130 S. Ct. at 2625.

74. *Id.* (emphasis added).

75. *Id.*

76. In the case of the pagers at issue in *Quon*, a log-on banner could have taken the form of a message that would have displayed upon removing the pager from being recharged and that would have had to be accepted through a click by the user in order for the pager to be operational.

## IV

Global Positioning System (GPS) monitoring is a rapidly growing form of surveillance.<sup>77</sup> What might the contemporaneous agreement favored in this Article over an in-advance agreement look like in the GPS monitoring context?

The log-on banners discussed above provide a ready analogy. If a government employer wished to engage in GPS monitoring of an employee's vehicle location during work hours and proposed to rely on employee agreement to avoid any potential Fourth Amendment challenge to such monitoring, the employer could include a daily log-on requirement before a GPS would activate. (The GPS being activated could be part of the employee's being "clocked in" for work.) By analogy to the discussion above, such a log-on requirement would be on far surer ground than an in-advance agreement at the start of employment to any GPS or other vehicle monitoring the employer might or might not decide to undertake in the future. At the same time, in using such a daily GPS log-on requirement, government would be preserving its ability to utilize the tool of agreement in managing its workplace.

Consider what would happen if, instead, even such a daily log-on requirement were found to be insufficient—most likely on grounds of voluntariness<sup>78</sup>—for a finding of "consent" under the Fourth Amendment. Although such a legal outcome might be either good or bad on balance—a normative question not addressed in this Article—such a result would produce a very significant impact on government operations. By contrast, targeting only in-advance agreement would, as a descriptive matter, impose far more modest costs on the structure of the government workplace.

It remains to consider an important potential limit on the daily log-on approach. If a government employer used a daily log-on approach in connection with its GPS monitoring, or in one of the other contexts discussed above, but at the same time let it become universally known that in fact it never monitored vehicles' whereabouts in any way—or computer or pager use, as the case might

---

77. See, e.g., *United States v. Jones*, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).

78. See *supra* note 6 and accompanying text.

be—then the daily agreement would arguably start to be characterized by the same type of uncertainty as that which exists under an in-advance agreement. In the terminology of express versus implied agreement, the employer’s publicization of its total lack of monitoring activity could cause the express daily agreement to be supplanted with a new implied in-advance agreement under which monitoring—as in *Simons*—might or might not occur at some point down the road; indeed, the implied in-advance agreement could even be one under which monitoring was not allowed at all. As noted above, however, the focus of this Article is on express agreement—a context that does not present the many additional interpretive and other complexities that arise with implied agreement. (To give just one example, with implied agreement in the workplace setting it often becomes necessary to determine whether a particular supervisory employee had authority to bind the employer to an implied agreement; if, for instance, a supervisory employee conspicuously and routinely avoids entering subordinates’ offices under any circumstances, asserting that offices are “private” and should never be entered by anyone but their rightful occupants, then is the employer bound by such an understanding?) Focusing in the first instance on express agreement allows one to bracket such further complexities and, it is hoped, permits the emergence of a clear understanding of the important distinction between in-advance and contemporaneous agreement. However, with the inexorable progression from the GPS technology at issue in *United States v. Jones*<sup>79</sup> to technologies—such as facial recognition software—that allow tracking of individuals without their use of any sort of mediating device or tangible object (to which an express agreement might be attached),<sup>80</sup> the importance of implied agreement is likely to grow with time and, accordingly, presents a compelling subject for future work on the role of agreement under the Fourth Amendment.

---

79. *Jones*, 132 S. Ct. 945.

80. See, e.g., Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 409 (2012) (“[F]ocusing on the physical placement of the GPS device ignores the growing body of tracking technologies that make no contact with the individual.”).

## V

This Article has sought to disaggregate in-advance and contemporaneous express agreement, but nothing in the analysis offered here suggests that even the latter form of agreement must necessarily be given a dispositive role in Fourth Amendment doctrine. That such agreement is often on surer footing than in-advance agreement should not be mistaken for the broader claim, for just as the young and inexperienced friend of the defendant in *Schneckloth v. Bustamonte* apparently gave his contemporaneous agreement to a police search because he feared what would happen to him if he refused,<sup>81</sup> government employees may give contemporaneous agreement automatically and largely involuntarily out of a fear for their livelihoods in the event of a refusal.<sup>82</sup> This Article's hope, however, is that understanding the special, additional limitations that attach to in-advance agreement will allow for more considered analysis of in-advance agreement's proper role in Fourth Amendment analysis.

---

81. Appendix E: Excerpts from Reporter's Transcript at 32, 37-39, *Schneckloth v. Bustamonte*, 412 U.S. 218 (1973) (No. 71-732) (individual who gave his agreement to the challenged police search was about twenty years of age at the time of the agreement); Tracey Maclin, *The Good and Bad News About Consent Searches in the Supreme Court*, 39 MCGEORGE L. REV. 27, 28 (2008) (observing that "a police 'request' to search a bag or automobile is understood by most persons as a 'command'" rather than an inquiry that leaves its recipient free to do as the recipient pleases).

82. Indeed, it is intriguing to note that none of the leading Fourth Amendment workplace drug testing cases has seemed to involve contemporaneous agreement. The distinctively personal nature of drug testing—in which the employee performs "an excretory function traditionally shielded by great privacy" in the presence of an employer monitor, *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 626 (1989)—may make salient the normative limitations on even contemporaneous agreement.

Copyright of William & Mary Law Review is the property of William & Mary Law Review and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.