A FRESH START: SURVEILLANCE TECH AND THE MODERN LAW FIRM

TITUS R. WILLIS†

ABSTRACT

The legal community is rapidly evolving: firms are more beholden to clients than ever, associates are growing more competitive with one another, and younger firm employees are more willing than ever to subject themselves to surveillance from their employers. These evolutions come alongside a boom in surveillance technology. Tech companies now provide services that can track every keystroke a lawyer makes on a company computer, analyze the content of their computer screens, or even develop algorithms to measure employee productivity.

How does the modern law firm respond to these new technologies? How do they weigh their obligations to clients with the privacy considerations of their employees? This Note examines these key questions and makes a comment about the honor of the legal profession along the way.

INTRODUCTION

Christopher Anderson had the beginnings of an impressive legal career: *summa cum laude* in his law school class, then several years as an associate at Kirkland & Ellis, then a partnership at Neal, Gerber & Eisenberg in Chicago.[1] But Anderson never admitted that, at each stop, he had padded his hours, such that his billed time amounted to 125 percent of his actual work time.[2] When he finally self-reported in 2018, Anderson had defrauded 100 clients of over $150,000 in billables after seven years at two firms.[3] His firm fired him and repaid the aggrieved clients, but the damage was done—one more drop in an ocean of bill-padding incidents; one more argument in the public's case against lawyers.[4]

Overbilling has plagued the legal community since billing itself began. Even in the Middle Ages, poets chided lawyers for their proclivity to overcharge,[5] calling them "not psalmists, but harpists of Satan" and,

† Duke University School of Law, J.D. expected May 2021.

[1] "Christopher Anderson," LINKEDIN, https://www.linkedin.com/in/christopher canderson/ (May 11, 2020).

[2] Debra Cassens Weiss, *Former BigLaw lawyer inflated hours because of perceived billing expectations, ethics complaint says*, A.B.A. J. (Jan. 22, 2019, 7:30 AM). www.abajournal.com/news/article/former-biglaw-lawyer-inflated-hours-because-of-perceived-billing-expectations-ethics-complaint-says.

[3] *Id.*

[4] *Id.*

[5] I could not cite this history without acknowledging that these accusations were often motivated, undoubtedly, by anti-Semitic tropes.

more straightforwardly, "merchants of the Devil."[6] Today, most lawyers admit to overbilling from time to time, not by claiming undone work, but by performing unnecessary tasks.[7] Firms only tend to catch the patently absurd ones. But the brunt of known incidents are self-reported—perhaps eighty percent of all documented misconduct comes from contrite lawyers with guilty consciences[8]—which means that even the most sophisticated firms rely on the "honor system" in one of the world's most famously dishonored professions.

The type of overbilling that Anderson practiced is common enough, even if firms aren't likely to detect it without thorough investigation. Instead of simply conjuring hours he had not worked out of thin air, Anderson billed slightly above every timeframe; he worked in increments that are almost invisible even when an attorney is sitting in the office, appearing diligent.[9] For example, if Anderson spent 0.7 hours—forty-two minutes—reviewing documents, he would bill 0.9 hours—fifty-four minutes. The seemingly subtle twelve-minute discrepancies become more obvious as they pile on top of each other throughout the day; ultimately, Anderson logs off his work computer at 6:15 p.m., even though his billables suggest he must have stayed on until 7:30 p.m. Diligent firms could catch this kind of misconduct easily if they tried.

But Anderson's modern misconduct raises concerns about stealthier types of overbilling. To see why, consider this scenario: Anderson *does* stay at work until 7:30 p.m., and bills his hours accordingly, yet his work for clients throughout the day is sporadic. Every twenty minutes, he takes a five-minute break to check his phone—if his firm tracks all devices on its WiFi network, perhaps he uses data, or perhaps he reads an article he downloaded at home. Perhaps he keeps a copy of the *Chicago Tribune* under his desk and tries to piecemeal his way through the crossword. Regardless, his computer screen is on, and the documents he claims to have reviewed are indeed on his screen for the hours he suggested. Anderson has charged the client 125 percent of what he should have but appeared entirely above-board.[10] How can clients be certain that firms guard against overbilling when this particular breed is imperceptible to traditional computer surveillance methods?

To address these concerns, law firms will likely follow other sophisticated businesses into a new level of employee surveillance,

---

[6] John A. Yunck, *The Venal Tongue: Lawyers and Medieval Satirists*, 47 A.B.A. J. 267, 268–69 (1960).

[7] Nathan Kopel, *Study Suggests Billing Abuse*, WALL ST. J. (May 1, 2007, 9:04 AM), http://blogs.wsj.com/law/2007/05/01/study-suggests-significant-billing-abuse/.

[8] Interview with Prof. Amy Richardson, Senior Lecturing Fellow, Duke University School of Law, in Durham, N.C. (Nov. 23, 2019).

[9] *See* Weiss, *supra* note 2 (explaining that the increments were gradual and went unnoticed).

[10] The only way to police this behavior, without appropriate technology, is to place an assistant in each lawyer's office to assure that they are working precisely when they suggest they are working, which elicits a host of efficiency and privacy concerns beyond the scope of this Note.

potentially altering the firm's landscape as a workplace forever. The companies that make computers, WiFi, and email servers now have the capability to compile the data their users generate, and some have begun selling that data (branded as "workplace analytics") to their corporate customers.[11] While most lawyers at sophisticated firms have known for years that their supervisors could track their emails, these new analytics go deeper. For the right price, a firm could purchase an ultra-specific look at each employee's daily activities.[12] The newest tech allows for companies to track employee productivity in far more precise ways: essentially, everything an employee does in her office or does while hooked up to a company server could come under scrutiny.[13]

Different parties in the legal services economy might respond differently to these advancements. Law firms concerned about keeping ethics violations at bay might rejoice at the advent of workplace analytics, but they also may not want to hire more tech help to manage all the data. Clients who demand transparency and productivity from their legal fiduciaries might demand that billing be as thoroughly vetted as technologically possible. Firm employees who are protective of their personal data and workplace habits might rightly bristle at this level of scrutiny. This final group's morale is essential to the profession for obvious reasons: if law firms already have a poor reputation for work-life balance, how much less attractive will they be for the brightest young minds if every firm must promise its demanding clients full-time surveillance?

This Note will discuss the challenges facing firms that might consider utilizing new technologies to increase surveillance of their billing employees. First, it will precisely define the new technologies—how they work and what they can accomplish for a business of any kind. Second, it will delve into the ethics rules that guide both firm and attorney activity concerning overbilling. Third, it will examine a firm's obligations to its employees (*vis-à-vis* employment and data privacy law), articulating the tension a firm should feel between these rules and the ethics rules. Fourth, it will assess the potential of this technology flowing downstream from the most sophisticated firms today to a broader swath of firms in the future, along with the possibility that clients demand that their firms purchase these technologies. Finally, the Note will propose that firms, firm employees, and clients implement "surveillance regimes"— an amenable solution to overbilling.

I. NEW TECHNOLOGY

Tech companies have already begun marketing workplace analytics to their corporate clients. Microsoft Corp., for example, monitors its employees' email correspondence, server chats, and virtual meetings to

---

[11] Sarah Krouse, *The New Ways Your Boss Is Spying on You*, WALL ST. J. (July 19, 2019, 5:30 AM), https://www.wsj.com/articles/the-new-ways-your-boss-is-spying-on-you-11563528604?mod=DJCP_pkt_ff.
[12] *Id.*
[13] *Id.*

gauge productivity.[14] It recently used its own software to offer that same service to Macy's, Inc., whose employees use Microsoft products at work.[15] Freddie Mac also availed itself of Microsoft's analysis to determine how frequently its employees took meetings and how many of those meetings might have been unnecessary or redundant.[16] These companies are but a couple of the tens of thousands of customers to whom Microsoft could offer its workplace analytics services.

Moreover, third-party analytics firms can utilize modern software technology to conduct research for businesses. That's precisely how TrustSphere contracted with McKesson, a pharmaceutical corporation, to understand why some McKesson departments have higher turnover rates than others.[17] TrustSphere analyzed over 130 million emails to determine how frequently and quickly employees in certain departments corresponded, ultimately concluding that higher internal correspondence rates promoted cohesion within a department.[18] And firms like TrustSphere are discovering more ways to measure employee behavior. According to Sarah Krouse of the *Wall Street Journal*, "Companies are increasingly sifting through texts, Slack chats[19] and, in some cases, recorded and transcribed phone calls on mobile devices."[20] Startup Ambit Analytics even offers workplace analytics based on conference room audio, where companies can discover which employees' voices are most persuasive and authoritative in a collaborative setting.[21] Law firms might have an especial interest in this technology: they could contract with Ambit or a similar firm to calculate which lawyers are the best negotiators.

Despite all these groundbreaking developments, however, none has more potential for overbilling accountability than the computer activity analysis offered by Teramind. This third-party analytics company boasts over 2,000 employers in its clientele.[22] Its services include "a suite of software that can take a live look at employees' screens, capture real-time keystrokes, record video of their activities and break down how they spend their time."[23] Teramind even uses an algorithm to categorize employee hours on a sliding scale from "productive" to "unproductive,"

---

[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] Slack is an instant-message communication platform that also provides file-sharing, archiving, and searching services for teams; Its parent company, Slack Inc., has a market capitalization of almost US$16 billion. Slack Technologies, Inc., BLOOMBERG, https://www.bloomberg.com/quote/WORK:US (last visited Mar. 28, 2020.)
[20] Krouse, *supra* note 10.
[21] *Id.*
[22] *Id.*
[23] *Id.*

primarily based on keystroke frequency.[24] Teramind has also developed an insider risk program to protect attorney-client privileged information and work product sent abroad.[25] Clearly, the company believes law firms are in the market for their services.

Law firms are indeed perfect candidates for Teramind's analytics. Billing hours to clients is the backbone of their business, and clients are exceedingly wary of law firms overbilling them. Consider, for example, Christopher Anderson's misconduct: a service like Teramind could have helped either of Anderson's employers catch him before he could spend seven years defrauding clients out of $150,000, and the firms would have maintained a reputation of diligence and forthrightness with clients. Even Anderson might have fared better under this kind of surveillance, because if he were outed as a first-year associate instead of self-reporting as a partner, his supervisors might have allowed him to keep his job and salvage his reputation.[26]

Given the novel nature of these employee monitoring innovations, however, the technology might take some time to round into form. New tech often takes time and multiple models before it becomes an efficient "final" product. Even multibillion-dollar entities like Microsoft will struggle to keep all of their new tech bug-free, and startups frequently take even longer to work out the kinks due to their operations' relative size. Over time, these products will become more and more reliable—and cheaper, too.

II. ETHICAL OBLIGATION TO CLIENTS

The law on overbilling while doing hourly-rate work is straightforward: any lawyer who pads her hours beyond a certain point violates the ethics rules. The American Bar Association established a bright-line standard on this issue a quarter-century ago, stating that, in the hourly-rate context, "A lawyer may not bill more time than she actually spends on a matter, except to the extent that she rounds up to minimum time periods (such as one-quarter or one-tenth of an hour)."[27] And if lawyers were wont to question what precisely was meant by "minimum time periods," the ABA followed up this statement in 1996 by specifically prohibiting minimum time periods that are "unreasonably large or are used in an abusive manner."[28] Examples of unreasonableness follow: "Two

---

[24] *FAQ*, TERAMIND, https://www.teramind.co/product/faq (last visited January 20, 2021).

[25] *Teramind for Legal Overview*, TERAMIND, https://www.teramind.co/solutions/industry/law (last visited January 20, 2021).

[26] It stands to reason that a firm would be more lenient with misconduct from an inexperienced first-year associate than an equity partner who has been systematically overbilling for almost a decade.

[27] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 379 (1993) (discussing billing for professional fees, disbursements, and other expenses).

[28] *Ethics Tip of the Month, February 2014*, A.B.A. J. (2014). https://www.americanbar.org/groups/professional_responsibility/services/ethicssearch/ethicstipofthemonthfebruary20140/.

fifteen-minute charges for two five-minute calls within the same fifteen-minute period seem inappropriate."[29] Lawyers understand that there are certain lines they ought not cross. After all, overbilling is not some ineffable *mala prohibitum* rule; it is fundamentally unethical and immoral to grossly overcharge one's clients. This shouldn't be hard.

Yet, most firms, especially larger ones, struggle to keep their attorneys accountable for non-obvious overbilling practices. Scholar Ronald Rotunda addresses the fact that overbilling has become especially prevalent in "big law" offices.[30] As the size and anonymity increase in these firms, argues Rotunda, accountability goes down:

> Several decades ago, when law firms were much smaller, a partner might be a little reluctant to do something that was ethically dubious (e.g., padding his legal bills) because of a fear that if his client complained and his partners discovered what he had done, they would forever look down upon him. … The moral calculus changes when you do not even know the names of your partners or what they look like. There is less fear of shame, particularly when your rank and salary within the law firm depends on billing hours and keeping your clients happy.[31]

Lisa Lerman, director of the Law and Public Policy Program at the Columbus School of Law, reiterates Rotunda's "rank and salary" thesis:

Many lawyers are preoccupied with gaining power within their law firms and with expanding their own incomes. For some lawyers, income is the clearest measure of their status. Preoccupation with money tends to have a corrosive effect on integrity. For some people, the desire for wealth leads to dishonesty because it's easier to expand your income more quickly if you don't bother about legal niceties.[32]

Lerman[33] and Rotunda[34] cite evidence that attorneys are overbilling more aggressively—and more egregiously—than ever before. These diagnoses of the high-achieving lawyer's psychosis matter because they identify the root of the overbilling problem: internal competition for status and bonuses. The growing trend of overbilling has led some firms to hire professional auditors to scrutinize their employees' bills. Since the 1990s, third-party companies who promise to review suspect legal bills have become increasingly popular.[35] State bar associations express

---

[29] *Id.*

[30] *See generally* Ronald D. Rotunda, *Why Lawyers Are Different and Why We Are the Same: Creating Structural Incentives in Large Law Firms to Promote Ethical Behavior-In-House Ethics Counsel, Bill Padding, and In-House Ethics Training*, 44 AKRON L. REV. 679, 686 (2010).

[31] *Id.*

[32] Lisa Lerman, *The Slippery Slope from Ambition to Greed to Dishonesty: Lawyers, Money, and Professional Integrity*, 30 HOFSTRA L. REV. 879, 880–81 (2002).

[33] *Id.* at 887–88.

[34] *Id.* at 687–88.

[35] For scholarship on the advent of legal billing, see Claire Hamner Matturro, *Auditing Attorneys' Bills: Legal and Ethical Pitfalls of a Growing Trend*, 73 FLA.

concerns about the procedures and ethics of these non-legal organizations, especially since their presence might spur dubious litigation, threaten attorney-client privilege, or harm the legal profession's reputation even further.[36] However, bar associations also acknowledge that these firms should be allowed to do their work so long as they do not impinge on attorney-client privilege without client consent.[37]

Ultimately, state bars welcome technological advances that allow their members to better serve the first principles of legal service. A lawyer is, fundamentally, "a representative of clients"[38] who must always "provide competent representation" to those clients.[39] To maintain his status as a competent representative, the ABA Model Rules demand that a lawyer "should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*."[40]

Overbilling denotes incompetence because it does the exact opposite of what a competent representative would do. Instead of efficiently taking care of a client's business as a trusted fiduciary, the overbiller costs clients unnecessary money and conveys untruths to the client about the services he provided. An analogue in another field is Ponzi schemers: how could one reasonably say that Bernie Madoff was a competent handler of his investors' money when his actions clearly demonstrated that he actually cost them what they entrusted him with?[41]

It follows that, since overbilling is an incompetent representation of clients, firm partners who oversee the billings have an obligation to at least consider "relevant technology" that could help them represent these clients more competently. This is the essence of the ethical argument for acquiring workplace analytics: a firm that ignores these technologies is willfully failing to do everything in its power to do right by its clients, and failure to do right by one's clients is, by definition, incompetent lawyering.

Of course, there are financial incentives to consider when contracting for these services. Smaller firms could feasibly argue that their overhead costs are already too high to justify hiring one of these companies to scrutinize their employees further—costs that might ultimately pass down to the clients in heightened hourly rates. This argument gets weaker, however, as the firm's profits grow. In her article

---

B. J., no. 5, 1999, at 14. For a modern example, *see* LEGAL BILL AUDIT, https://legalbillaudit.com (last visited Apr. 4, 2020) (advertising that a third-party auditing service that analyzes bills over $50,000 from clients to determine if the client has been overcharged).

[36] *See* Matturro, *supra* note 35.

[37] *See id*. at 18 (noting that, in insurance defense contexts, an insurance company may hire an auditor to examine their legal bills who could require investigation into the specifics of an insured's privileged communication with an attorney).

[38] *See* MODEL CODE OF PROF'L RESPONSIBILITY Preamble (AM. BAR ASS'N 2018).

[39] *See* MODEL CODE OF PROF'L RESPONSIBILITY r. 1.1 (AM. BAR ASS'N 2018).

[40] MODEL CODE OF PROF'L RESPONSIBILITY r. 1.1 cmt. 4 (AM. BAR ASS'N 2018) (emphasis added).

[41] For background on Bernie Madoff, see *Bernard L. Madoff*, N.Y. TIMES, https://www.nytimes.com/topic/person/bernard-l-madoff (last visited Apr. 4, 2020).

on big-firm greed, Lerman notes that profits are continually increasing as firms consolidate into one another.[42] At some point, earnings become so outsized (and hourly rates become so high) that partners at the most affluent firms in the country should not be afraid to suffer a minor setback if it means restoring confidence, for both their clients and the public, that lawyers are indeed billing their customers with integrity.

III. FAIRNESS TO EMPLOYEES

American employees have precious few rights when it comes to data privacy. For now, firms' concerns regarding employee fairness might be more normative; if firms are regularly watching every first-year associate's keystrokes throughout the day, they might make the legal profession unattractive. Given the high supply of graduated law students relative to firm demand, perhaps this development would be a welcome thing for the profession. Perhaps, at present, firms have nothing to worry about here.

But this is an evolving area of the law. Employment privacy law promises to develop significantly as these technologies become more common in American workplaces, and courts have suggested that public opinion will play a key role in understanding what degree of surveillance is beyond the pale. As time passes and views on employers' high-tech behaviors shift, courts will allow those opinions to guide them. Simultaneously, courts can build canons that distinguish acceptable and unacceptable employer conduct. It is too soon to tell, but one could argue that these courts will look to older notions of privacy and intrusion as they take these steps.

A. Privacy Torts

Employee privacy law dates back to "privacy torts" that arose around the turn of the century. Privacy rights had garnered minimal discussion in the legal community until 1890, when future Supreme Court Justice Louis Brandeis and his firm partner Samuel Warren wrote a groundbreaking article, "The Right to Privacy," in the *Harvard Law Review*. Spurred on by an increasingly aggressive journalist class, Brandeis and Warren argued that to protect the person, there needed to be a "right to be let alone."[43] These rights were not merely contractable, or based on some duty of trust, but were "rights against the world" for which "the elements [of] demanding redress exist"[44] in tort.[45] The common-law mechanisms of 1890 could already protect privacy rights; judges simply needed to fashion them to use for those purposes.

Although the context of Brandeis and Warren's article differs significantly from, for example, Teramind's employee surveillance system, the logic they utilized applies to even the most cutting-edge tech. The authors asserted that U.S. common law must "protect the individual

---

[42] *See* Lerman, *supra* note 32, at 883–84.
[43] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).
[44] *Id.* at 213.
[45] *Id.* at 219.

from invasion either by the too-enterprising press, the photographer, or *the possessor of any other modern device for recording or reproducing scenes or sounds*."[46] Perhaps the article itself spent most of its time focused on Gilded-Age paparazzi, but the basic premise it espoused—that individuals using the latest technology should not be able to unreasonably track your private behaviors—make sense in any historical moment. That Warren and Brandeis were discussing enterprising newspapers 120 years ago does not effect the broad implications of their argument; if anything, an algorithm that tracks your computer screen all day, every day (which could be used to fire you) seems *more* intrusive on individual privacy than a single picture taken by an overbearing journalist of someone in their home.

Moreover, the standards espoused by the article have gained widespread acceptance in the legal community over the years. The Restatement (Second) of Torts mentions the right to privacy by name and introduces four specific wrongs that violate the right: (1) unreasonable intrusion on the subject's private life; (2) appropriation of name or likeness, (3) unreasonable publicity of private life, and (4) publicity that places the subject of the surveillance in a false light to the public.[47] While the latter three rights have little to do with employers monitoring their employees, the first—intrusion—might prove essential, given certain interpretations.

B. Current Interpretation of Right Against Intrusion

Some of the key principles underlying the modern intrusion tort come from the 1987 case *O'Connor v. Ortega*, where the Supreme Court liberally construed an employee's right against searches from his employer.[48] Napa State Hospital placed Ortega, one of its employees, on administrative leave for suspicion of impropriety, then searched his office for evidence (without his consent) while he was on leave.[49] The Court held the public hospital liable for this employee search under the Fourth Amendment, because they violated Ortega's "reasonable expectation of privacy."[50] In so holding, the Court emphasized that:

> Not everything that passes through the confines of the business address can be considered part of the workplace context. . . . While whatever expectation of privacy the employee has in the existence and the outward appearance of the luggage is affected by its presence in the workplace, the employee's expectation of privacy in the contents of [an employee's personal property] is not affected in the same way. The appropriate standard for a workplace search does not necessarily apply to a piece of closed

[46] *Id.* at 206 (emphasis added).
[47] RESTATEMENT (SECOND) OF TORTS § 652A.
[48] 480 U.S. 709 (1987).
[49] *Id.* at 713–14.
[50] *Id.* at 718 ("The Court of Appeals concluded that Dr. Ortega had a reasonable expectation of privacy in his office, and five Members of this Court agree with that determination.").

> personal luggage, a handbag, or a briefcase that happens to be within the employer's business address.[51]

Though the Supreme Court has not commented on this matter, some circuit courts have argued that the *O'Connor* presumption, at least with respect to public entities, against searching employee's personal items can be refuted if the employer publishes a policy reserving the right to conduct such searches.[52]

Applying the reasoning in *O'Connor* to modern cases of electronic employee surveillance provides some answers to how far employers can go. Most fundamentally, an employee possesses a reasonable expectation of privacy against a search of her personal effects that might be refuted by a stated employee policy allowing such searches. Public employees who use their personal cell phones to surf the internet on company property, or to use state government wi-fi, might compare these devices to the "personal luggage" referenced in *O'Connor*, such that employers cannot search them amid overbilling investigations. Regardless, *O'Connor* predates the internet and most modern forms of communication; today's Court might allow itself to develop an entirely new canon of law for electronic surveillance if they take on such a case.

Federal and state statutes impose burdens on employers, but the burdens rarely pose material challenges for employers who want to study employee conduct. For example, some states demand that employers alert their employees when surveillance occurs, but once the employer makes this notification, it can begin its surveillance practices in earnest.[53] The Electronic Communications Privacy Act of 1986 (the "ECPA") prohibits the interception of many kinds of electronic communication, including emails, Slack chats, and instant messages, but offers exceptions for employers when (1) the employee consents to the surveillance, or (2) when the employer provides the system through which the communication occurs.[54] While some state laws supplement these lax requirements with slightly more stringent ones,[55] the general tone of the employee electronic

---

[51] *Id.* at 716.

[52] *See, e.g.*, *Muick v. Glenayre Elecs.*, 280 F.3d 741 (7th Cir. 2002) (holding that a government employer's reservation of the right to inspect laptops left no room for an employee to have a reasonable expectation of privacy when the search occurred); Biby v. Bd. of Regents of Univ. of Neb. at Lincoln, 419 F.3d 845 (8th Cir. 2005) (holding that if a public university's computer policy permits searches, no reasonable expectation of privacy exists for students who are subject to such searches).

[53] *See, e.g.*, Del. Code Ann., Tit. 19, § 705; Conn. Gen. Stat. Ann. § 31-48d.

[54] *See* 18 U.S.C. §§ 2510 to 2511. The statute also excepts employee surveillance that an employer conducts on devices used within the "course of ordinary business," but only when such surveillance occurs non-continuously. The noncontinuity requirement precludes tech like Teramind and Microsoft's from enjoying the exception.

[55] *See, e.g.*, Maryland Wiretap & Electronic Surveillance Act, Md. Code Ann. § 10-401 through § 10-414 (providing that, to lawfully intercept communication from its employees, employers must have the consent of both the sender and the receiver of the communication); PUBLIC UTILITIES COMMISSION OF THE STATE OF CALIFORNIA, GENERAL ORDER 107-B (adopted July 1, 1983) (providing that

surveillance statutes is clear: as soon as employees are properly notified of the policy, the surveillance can commence. Moreover, these laws only cover communications between two parties; employees' private activities (like checking NFL box scores) on employer systems (like a work computer or work wi-fi) are fair game for surveillance.

On the whole, current U.S. law on data privacy in the workplace suggests that employees have minimal rights against surveillance. Perhaps employees enjoy a default right to privacy under *O'Connor* and the ECPA, but this right can easily be abrogated by employee consent to surveillance—which, in the real world, tends to happen by employees absentmindedly clicking through a series of warnings on a computer screen before logging in. If an employee felt violated or trespassed upon by a surveillance regime, she could reject it by quitting the job, but this is not exactly an equitable solution to the privacy concern. For most people, especially young lawyers who sometimes spend hundreds of thousands of dollars to earn the right to graduate law school and get admitted to a state bar, the option to resign from a job at which you feel too closely watched is fiscally unconscionable. Law firms can lay out their terms, point a gun at first-year associates' heads, and dare them not to sign the dotted line. Most will sign. Those who don't give their employers *carte blanche* for surveillance are increasingly unlikely to get a position in a profession where clients are up the food chain, negotiating with firms, brandishing an even more lethal weapon.

C. Present Normative Challenges

The only real obstacle in a firm's way, then, is not based in common law or statutes, but in a much more on-the-ground difficulty: that potential employees will not want to work at a place where their supervisors have promised to clients that every associate's move could come under scrutiny. This development could, at least in theory, reach all the way down to college upperclassmen if employee surveillance in legal jobs is significantly higher than in other occupations. Law already has notorious problems with sleep deprivation, alcoholism, depression, and poor work/life balance—not quite an encouraging set of features for college students considering career paths. Adding increased surveillance onto those challenges might be enough to scare the best and brightest students away for good. If that transpires, clients will, ironically, receive inferior service in the long run.

But this argument could be refuted in at least four ways. First, the legal market is already oversaturated. A lower quantity of lawyers could mean fewer firms feel the need to expand, which would lead them to hire fewer associates.[56] Second, young people (who comprise the vast majority of the profession's new entrants) are less worried about data privacy than

---

monitored phone calls include a beep or some kind of verbal message to indicate the surveillance so those who speak after the notification have constructively consented to it).

[56] *See Lawyers*, BUREAU OF LABOR STATISTICS, https://www.bls.gov/ooh/legal/lawyers.htm (noting that "more students are graduating from law school each year than there are jobs available") [hereinafter LABOR STATISTICS].

older people (who comprise the vast majority of senior partners at firms where purchasing this technology might make sense). While recent studies suggest that both young and old have concerns about their traceable conduct in the modern age, a 2013 study shows that millennials consistently display less distrust in those who may be watching them.[57] Third, perhaps the people who get scared away due to increased surveillance were not the kind of people that the legal community needed to join its ranks anyway: those who are above reproach have less to worry about in terms of how they use their work-related information. Fourth, it is possible that even a significant increase in large law firms' employee surveillance measures would fail to make a ripple in the market since many of the most fundamental aspects of law practice are unknown to a surprising amount of law students.

Combine these counterarguments with the fact that employers enjoy in surveillance contexts, and the grass could not be greener for firms seeking to purchase these technologies. Even after a quarter-century with the internet and an extremely innovative tech industry, the legal markets are not yet resistant to unchecked employee surveillance. Law firms, who have a host of ethical obligations to clients, should at least take note of this reality and analyze surveillance opportunities while they are available.

D. Future Legal Concerns

At this juncture, firms seem to face few obstacles in imposing stricter surveillance regimes—they have essentially all the power over their employees—but this may not be the lay of the land for much longer. The Supreme Court took note of the role evolving public opinion might play in these cases while deciding *City of Ontario v. Quon*:

> Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. . . . [M]any employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency.. . . [The] law is beginning to respond to these developments, as some States have recently passed statutes requiring employers to notify employees when monitoring their electronic communications. At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve.[58]

In *City of Ontario*, the plurality cited this rationale as it expressly avoided making a broad constitutional conclusion about the rights public employees deserve under the Fourth Amendment. "A broad holding concerning employees' privacy expectations vis-á-vis employer-provided technological equipment might have implications for future cases that cannot be predicted," the Court said.[59] "It is preferable to dispose of this

---

[57] Hadley Malcolm, *Millennials Don't Worry about Online Privacy*, USA TODAY (Apr. 21, 2013), https://www.usatoday.com/story/money/business/2013/04/21/millennials-personal-info-online/2087989/.

[58] 560 U.S. 746, 759 (2010).

[59] *Id.* at 760.

case on narrower grounds."[60] But the fact that the Court suggested change on the horizon might not be the only worry employers have about surveillance in the coming years. If the public frowns upon more zealous surveillance, elected officials will respond in kind with statutes, and the reasonable-expectation standard adopted by the Court will allow the public to guide its decision-making on this issue as well.

IV. FUTURE DOWNSTREAM ADVANCEMENTS

As time passes, individual tech will become more affordable and accessible to less affluent firms. "As technology gets more advanced, prices drop and products get better," says Matt Rossoff of the Business Insider.[61] This is a self-evident truth for the twenty-first century: name the groundbreaking innovation of ten years ago and find most of those once-heralded products sitting in a landfill somewhere, or on sale in a secondary market for an infinitesimal fraction of the original price. A high-end innovation in today's market like Teramind will likely be run-of-the-mill by 2030.

As the tech continues to advance and increasingly invasive employee surveillance services become more widespread, clients will likely demand that law firms intensify their own monitoring practices. Today's clients are as empowered as ever; the consolidation of major firms and the lessons learned from the late-2000s financial crisis have made legal services a "buyer's market" like never before.[62] Thus, even if firms choose not to address innovations in employee surveillance now, their clients will undoubtedly begin to pressure them to do so as those services become more prevalent and more affordable.[63] No matter a firm's size, today is the day to face the tensions that heightened surveillance might create. From a business perspective, it is imperative to know about this service before clients start requesting it.

V. POSSIBLE SOLUTIONS

No firm can afford to simply ignore the innovations taking place in employee monitoring, but precisely what surveillance regime a firm should choose will depend on their current circumstances. Although each firm has countless idiosyncrasies, this Note lays out three general options that firms can take to prepare for the future while maintaining a healthy office environment in the present. After a firm chooses the general route it will take, it can tinker with the specifics to discover a more individually-tailored approach.

---

[60] *Id.*

[61] Matt Rosoff, *Why Is Tech Getting Cheaper?*, WORLD ECON. F. (Oct. 16, 2015). https://www.weforum.org/agenda/2015/10/why-is-tech-getting-cheaper/.

[62] *See* JORDAN FURLONG, LAW IS A BUYER'S MARKET (2017); *see also* LABOR STATISTICS, *supra* note 56 ("Clients are expected to cut back on legal expenses by demanding less expensive rates and scrutinizing invoices.")

[63] Interview with Amy Richardson, Senior Lecturing Fellow, Duke University School of Law, Durham, N.C. (Nov. 23, 2019).

A. Avoid the Technology (for now) and Continue Standard Surveillance Procedure.

The argument for this course of action is simple: the long-run disadvantages of paying for cutting-edge workplace[64] analytics would outweigh the benefits. Perhaps the advantages do indeed outweigh the disadvantages in the immediate present, especially for a firm whose clients are not yet aware of the fact that every single lawyer in the firm could have their activities tracked throughout the office, from hours graded on productivity to voice inflections in conference-room strategy meetings. As mentioned in Part V *supra*, most clients will not be unaware of this technology for much longer. Still, they are unaware now—so what's the harm of waiting a few more years before seriously considering implementing the technology?

This surveillance regime makes the most sense for firms whose clients are probably several years away from learning about monitoring innovations. These types of clients are likely less sophisticated and probably do not have the funds to scrutinize their law firm's billing procedures; further, they are probably paying a lower hourly billable rate than more sophisticated clients, whose overbilling risk is higher. While firms who serve these clients still ought to convey that they are serious about employee monitoring and accurate billing, it's not yet time to splurge for a new product that might take a few years to be free of bugs and kinks. So long as these firms have earned a positive, ethical reputation with their clients and the clients are not focused on discovering new ways to scrutinize billables, the *status quo ante* will do just fine.

B. Purchase the Technology and Only Punish the Egregious Overbilling Cases.

This approach attempts to square the challenges of evolving with an ever-changing tech market, slaking an increasingly demanding client base, and respecting the employee behavior status quo leading to significant financial success for thousands of sophisticated law firms across the country. Under this surveillance regime, firms would proclaim to clients that they have redoubled their efforts to preserve integrity in their billing practices by implementing the latest, most innovative monitoring tech available. However, on the inside, the frequency of punishment remains essentially the same: self-reporting employees can still face discipline, of course, but only the most brazen overbilling offenders receive punitive treatment from the firm. Perhaps a firm adopting this strategy might even hold a brief seminar with their employees where they explain the new technology, what to avoid, and when bill-padding will rise to a level that requires disciplinary measures. Firms who adopt this solution successfully will leave both their clients and their employees at ease while solidifying their outward-facing reputation as above-board in their billing practices.

---

[64] Namely, the direct financial costs and employee discontent.

Firms who have strong relationships with sophisticated clients, and minimal history of billing issues, should embrace this approach. When these types of clients inevitably request to minimize their billing expenses as much as possible, their firms can reassure them that they are working with superior technology to assure that everything will continue to run smoothly. Coupling a loudly-proclaimed tech advantage with a relatively unaffected employee base makes sense for firms whose clients want advantages, and whose employees have already done well in their efforts to bill accurately. For firms with less-confident clients, or a significant history of bill-padding, purchasing the tech while essentially maintaining the same level of surveillance could be dangerous—it would not preserve confidence if the punishment system remains the same, and it would not make the employees behave any better. A firm in this latter state gains little to no cost advantage from buying the technology; moreover, they are not acting any more ethical just because they bought it.

C. After Extensive Communication with Lawyers and Other Billing Employees, Purchase the Technology and Establish Bright-Line Standards of Punishable Conduct, then Enforce Them.

This regime stresses transparency and communication—two crucial components of any new employee surveillance initiative. However, unlike the approach in section VI-B *supra*, this makes a concerted effort to enhance genuinely employee behavior and crackdown on overbilling. Firms might purchase Teramind's sliding-scale service and tell their employees that any productivity level below a certain point will result in heightened scrutiny on their file, with a system of increasingly strong penalties for repeat offenses. Or perhaps a firm could pay for Microsoft's analytics and tell employees that the firm reserves the right to examine every email they exchange. Regardless, the chief end of the process should be raising employee awareness so that every lawyer knows precisely what's expected of her.

Firms who choose this strategy will most likely have demanding clients and demanding employees—hardly a bad combination. Clients will find reassurance in adopting of the new technology and the heightened communication; employees will appreciate the fact that, while the firm is indeed "spying" on them, they know what to expect and what to avoid. Moreover, this plan has the benefit of actually being the *most ethical option*: it assures proper billing while giving employees a fair shake. Generally speaking, law firms will most competently serve their clients under this surveillance regime. While it might cost some money and put a bug of paranoia in some naïve associates' ears, it is clearly the best choice for the future for most firms that have reason to purchase the new technology.

CONCLUSION

The legal profession is unlikely to ever "solve" overbilling, and it has a similarly slim chance of making its jobs more attractive as clients have more leverage to demand compliance. But these realities do not exempt a law firm from incorporating new monitoring technologies into their standard employee surveillance procedure. When the ABA said in its

Model Rules that a lawyer was, first and foremost, "a representative of clients," it surely must have meant that prioritizing client interest was a lawyer's, or a law firm's, fundamental professional purpose. As companies like Microsoft and Teramind continue to develop their offerings, every firm in the country should pay attention and genuinely consider using them to help themselves be the best lawyers they can be.

Of course, employee rights matter as well—especially those of relatively helpless junior associates who might not be long for a profession that systematically spies on them. For every Christopher Anderson, many other young attorneys deserve to be treated with decency and only a reasonable amount of scrutiny. These recent law school graduates are already walking into positions that notoriously induce mental illness, alcoholism, and overwhelming stress. As this new horizon of employment law develops over the next few years, firms owe it to their field to be fair and understanding with their associates and to deemphasize their most destructively competitive earning and positional structures so that the temptation to pad bills is not so enticing.

Employee monitoring innovations could signal a fresh start for firms that have a reputation for incubating internal misconduct. Instead of fostering an environment where young associates like Christopher Anderson feel compelled to defraud clients to get ahead, firms can rebuild their cultures to focus on transparency, collegiality, and ethicality. That employees will be more closely monitored in the coming decades is almost inevitable. Firms can respond to this development by promising both their employees and their clients new incentive structures that comport with a transparent billing system. By doing so, our profession can not only evolve with the times and maintain client confidence but project a new, positive image of the lawyer's psychosis—a makeover we have sorely needed for centuries.