A System Under Artificially Intelligent Strain: Can Hatch Act Enforcement Handle AI Surveillance?

ALEX COMFORT*

TABLE OF CONTENTS

* J.D., Georgetown University Law Center (expected May 2026); Villanova University, M.A., 2023; Villanova University B.A., 2022.

INTRODUCTION

Did anyone truly know what a mouse jiggler device was prior to the COVID-19 pandemic? In the years since, as telework has become increasingly prevalent, people turned to mouse jigglers and other such devices to outsmart surveillance software called "tattleware"[1] or "bossware."[2] These devices essentially mimic mouse movement to prevent a computer from entering "sleep mode" in order to avoid software that monitors employees' screen time.[3] Surveillance software can monitor a variety of different employee activities, from detailed information on websites, apps, and files accessed, to seeing emails and messages sent by employees—all in real-time.[4] When employed to its full capacity, surveillance software can utilize cameras and microphones on employees' computers to listen and even watch staff at work.[5] Add artificial intelligence (AI) to the mix and things only get scarier. AI models are well-suited for the sort of surveillance employers crave—"[t]hey are efficient at counting and identifying the words typed in and websites visited; the number of emails sent; the number of steps taken in a warehouse; the number of bathroom breaks; [and] their length."[6] When employed to its maximum extent, the software is akin to someone looking over an employee's shoulder throughout the entire workday.[7]

Naturally, this raises troubling privacy concerns for all employees.[8] For federal employees specifically, the question of compliance with laws such as the Hatch Act races to the fore. The Hatch Act, designed to prevent political influence by the nation's federal civil service,[9] prevents most federal employees from engaging in political activities while "on duty" or actively working.[10] Even though the government is pursuing a government-wide return to work policy, ad-hoc

---

1. *See* Sofia Blum, *This $30 Mouse Jiggler Makes it Look Like You're Working When You're Not*, CNBC (Sept 2, 2022), https://www.cnbc.com/2022/09/02/how-to-use-a-mouse-jiggler-to-make-it-look-like-youre-working.html [perma.cc/E9LB-ZRTN].

2. *See* Megan Carnegie, *The Creepy Rise of Bossware*, WIRED (July 23, 2023), https://www.wired.com/story/creepy-rise-bossware/ [perma.cc/3RA3-W7YN].

3. *See* Blum, *supra* note 1.

4. Carnegie, *supra* note 2.

5. *Id.*

6. *See* Leonie Cater & Melissa Heikkilä, *Your Boss is Watching: How AI-powered Surveillance Rules the Workplace*, POLITICO (May 27, 2021) https://www.politico.eu/article/ai-workplace-surveillance-facial-recognition-software-gdpr-privacy/#:~:text=Experts%20warn%20that%20what%20looks,and%20personal/family%20life.%E2%80%9D [perma.cc/8AT6-5W5R].

7. *See* Thorin Klosowski, *How Your Boss Can Use Your Remote-Work Tools to Spy on* You, N.Y. TIMES (Feb. 10, 2021) https://www.nytimes.com/wirecutter/blog/how-your-boss-can-spy-on-you/ [perma.cc/55NB-S6A4].

8. *See, e.g.*, Carnegie, *supra* note 2 (providing an example of how Amazon employees are constantly monitored, even while on breaks including using the restroom).

9. Ian Hargreaves, *Hatching a Plan: Filling the Enforcement Gap in the Hatch Act and the Extraordinary Case of Kellyanne Conway*, 21 U.C. DAVIS BUS. L.J. 225, 229 (2021).

10. U.S. OFF. OF SPECIAL COUNS., *Federal Employee Hatch Act Information,* https://osc.gov/Services/Pages/HatchAct-Federal.aspx#tabGroup13%7CtabGroup32%7CtabGroup51 [perma.cc/6SH7-DEG6] (Nov. 24, 2024, 12:30 PM).

telework raises the question of what constitutes "on duty," especially if employees intersperse their workday with everyday tasks like running errands.

This note argues that the rise of AI-powered surveillance software will put extreme stress on the Hatch Act's current enforcement system if employed by the government to monitor federal employees' compliance with the law. AI software offers a level of comprehensive surveillance of employee actions that is impossible to obtain by traditional means. Despite this increased effectiveness, the use of AI raises concerns about reliability.

Part I will explore the current state of the Hatch Act by explaining its history, persons and actions covered by the Act, and the enforcement system as it stands today. Additionally, Part I will discuss the connection between the Hatch Act and the *Model Rules of Professional Conduct*, specifically Rule 8.4(c)[11] and 8.4(e)[12] which emphasize lawyer integrity and the importance of public trust in government.

Part II will explore the use of AI in the workplace and government. Specifically, it will discuss keystroke and facial recognition software as examples of the types of AI programs that would stress the Hatch Act enforcement system. Accuracy concerns inherent in keystroke and facial monitoring software from the private and public sector paint a concerning picture of how use of this software may artificially inflate reported Hatch Act violations.

Part III will discuss the impact of AI surveillance on the Hatch Act enforcement system. A case study of the IRS' tax return system—which faces stress from its use of automated data-driven software—will highlight the impact that a greater number of Hatch Act claims may have on the Office of Special Counsel (OSC), including how operational capacity considerations affect which claims are pursued.

I. THE CURRENT STATE OF THE HATCH ACT

A. HISTORY OF THE HATCH ACT

Officially titled "[an] Act to Prevent Pernicious Political Activities," the Hatch Act's passage followed a "decades-old effort" to separate political influence from the work of the nation's federal civil service.[13] Preceding the Hatch Act, the Pendleton Civil Service Act of 1883 effectively "curbed the role of political patronage" in staffing federal positions, in part by creating the Civil Service Commission to legally enforce the Act's provisions.[14]

The Hatch Act drew heavy inspiration from the Civil Service Commission, including prohibitions on federal employees from influencing election results by virtue of their role in the government.[15] The Civil Service Commission would eventually morph into the modern-day Merit Systems Protection Board (MSPB), which

11. MODEL RULES OF PROF'L CONDUCT R. 8.4(C) (2018) [hereinafter MODEL RULES].
12. MODEL RULES R. 8.4(E).
13. Hargreaves, *supra* note 9 at 229–30.
14. *See id.*
15. *See id.* (citing U.S. Civil Serv. Comm'n v. Nat'l Ass'n of Letter Carriers, 413 U.S. 548, 568–69 (1973)).

adjudicates Hatch Act enforcement claims.[16] The Hatch Act notably differed from the preceding Civil Service Commission insofar as it applied "broadly to nearly all federal employees."[17] The law was eventually amended to allow "most federal employees to be active in political management and political campaigns when off duty. . . ."[18]

B. PERSONS AND ACTIONS COVERED BY THE HATCH ACT

The Hatch Act's coverage is expansive, encompassing "any individual, other than the President and the Vice President, employed or holding office in—(A) an Executive Agency other than the Government Accountability Office; or (B) a position within the competitive service which is not in an Executive agency. . . ."[19] Covered employees are categorized into "less restricted" and "further restricted" designations, and are subject to different constraints respectively.[20]

Further restricted employees, typically those employed in intelligence and enforcement-type agencies, face the most stringent prohibitions.[21] The Act precludes these employees from working for or engaging in partisan political campaigns.[22] In addition, further restricted employees cannot wear or display partisan political items, contribute to partisan political entities, or post advocacy content on social media.[23] These restrictions persist for further-restricted employees even when they are away from their official workplaces."[24]

Less restricted employees, however, can engage in political activities if the activity "is not performed in concert with a political party, partisan political group, or a candidate for partisan political office."[25] By statute, less restricted employees do not work for the intelligence and enforcement agencies.[26] They enjoy greater latitude in that they are able to engage in partisan campaigns and hold office in political clubs or parties.[27] They may engage in partisan actions while off duty.[28] Off-duty less restricted employees can post political content on their social media[29] and engage in other expressive conduct without using their official title

16. WHITNEY NOVAK, CONG. RSCH. SERV., THE HATCH ACT: A PRIMER (2020).

17. Christopher Ligatti, *Everybody Knows: Amending the Hatch Act to End the Legal Fiction that Presidential Appointees are Apolitical*, 73 DEPAUL L. REV. 1, 6 (2023).

18. *Id.*

19. 5 U.S.C. §§ 7321-7326 [hereinafter Hatch Act].

20. CYNTHIA BROWN, CONG. RSCH. SERV., HATCH ACT RESTRICTIONS ON FEDERAL EMPLOYEES' POLITICAL ACTIVITIES IN THE DIGITAL AGE, 4 (2016) (noting that the President, Vice President, members of the armed forces, employees or those holding office in the District of Columbia, and employees in the legislative or judicial branches are not subject to the Hatch Act).

21. *See* U.S. OFF. OF SPECIAL COUNS., *supra* note 10.

22. *Id.*

23. *Id.*

24. Brown, *supra* note 20, at 6.

25. *Id.* (quoting 5 C.F.R. §734.402).

26. *See id.* at 4.

27. *See* U.S. OFF. OF SPECIAL COUNS., *supra* note 10.

28. *Id.*

29. *See id.*; Brown, *supra* note 20 at 7.

or publishing their political affiliation. [30] In general, employees are not allowed to engage in expressive conduct while on duty.[31]

C. TELEWORK AND HATCH ACT CONCERNS

The rise of telework in the post-COVID-19 era has led to questions about when an employee is considered "on duty" for purposes of the Hatch Act, especially if an employee is physically home while conducting federal work. The Office of Management and Budget, in a recent report to Congress, noted that as of May 2024, 10% of all federal employees work entirely remotely, and federal employees who are telework-eligible reportedly spent around 60% of their work hours in person.[32] Even though the federal government is returning to full-time in office work for the majority of federal employees, unique Hatch Act enforcement challenges related to telework remain. Employees will likely continue to participate in virtual meetings and engage in ad-hoc telework for emergencies.

What employees can or cannot do under the Hatch Act is in large part determined by whether they are "on duty" or not. Employees are considered "on duty" by virtue of their pay status rather than their physical location.[33] As a result, teleworking employees are still considered on duty for purposes of the Hatch Act.[34] Even when at home, teleworking employees are not permitted to use their personal accounts to post political messages on social media.[35] In addition, these employees must be careful to ensure they are not displaying campaign or partisan materials while videoconferencing for work purposes.[36] As the teleworking environment continues to evolve, agencies have been encouraged to develop clearer policies regarding computer usage and government equipment.[37]

D. HATCH ACT ENFORCEMENT

The Hatch Act enforcement system, as it stands, employs different enforcement mechanisms and agencies to ensure compliance across the large federal workforce. The Hatch Act is codified as 5 U.S.C. §§ 7321-7326.[38] The Act involves two different enforcement mechanisms, respectively triggered by whether

30. Brown, *supra* note 20 at 9.

31. *Id*. at 7–8.

32. Andrea Hsu, *Trump Seeks to End Telework for Federal Workers*, NAT'L PUB. RADIO (Jan. 21, 2025), https://www.npr.org/2025/01/20/nx-s1-5268852/trump-telework-executive-order-federal-workers [https://perma.cc/9LT7-6EC8]. President Trump has recently signed an executive order mandating the return of federal employees to in-person work, with carveouts for employees to remain in their work from home arrangement.

33. U.S. OFF. OF SPECIAL COUNS., HATCH ACT ADVISORY FOR TELEWORKING EMPLOYEES (2020).

34. *See id.*

35. Stephanie Rapp-Tully, *How Does Telework Affect the Hatch Act? Election Season Do's and Don'ts*, TULLY RINCKEY PLLC, (Oct. 18, 2022), https://www.tullylegal.com/our-firm/news/how-does-telework-affect-the-hatch-act-election-season-dos-and-donts/ [https://perma.cc/RZN8-MDEH].

36. U.S. OFF. OF SPECIAL COUNS., *supra* note 33, at 2.

37. Brown, *supra* note 20, at 10.

38. Hatch Act, *supra* note 19 (providing an exhaustive list of the different agencies and positions that further restricted employees are employed by).

the subject of the investigation is a presidentially-appointed and Senate-confirmed employee or not.[39] If the employee is part of the former group, then "disciplinary discretion [has traditionally been assigned] to the President."[40] For the latter group, disciplinary action is brought through the U.S. Office of Special Counsel to the Merit Systems Protection Board.[41] MSPB is a bipartisan organization consisting of three members appointed by the President and confirmed by the Senate.[42] The Board is nonpartisan, and no more than two members can be of the same political party.[43]

Special Counsel Dellinger, who served during President Biden's term, issued guidance updating OSC's enforcement procedure.[44] This shifted the allocation of Hatch Act cases involving White House staff to MSPB, limiting presidential discretion.[45] Arguing that Congress "wants the Hatch Act to apply to as many people as possible," Dellinger aimed to eliminate the class of employees that were subject to disciplinary action at the sole discretion of the president.[46] Dellinger additionally announced that OSC would continue to pursue violations by individuals who engaged in prohibited activity while a federal employee but who left federal employment prior to the commencement of an OSC investigation.[47]

Multiple bureaucratic agencies work alongside each other in the current enforcement system. The Office of Personnel Management, for instance, is responsible for issuing regulations regarding which activities are permitted and prohibited for federal employees.[48] Separately, the Office of Special Counsel independently investigates and prosecutes alleged violations of personnel law while also creating advisory opinions that federal employees rely on.[49]

One such personnel law that the Office of Special Counsel enforces is the Hatch Act.[50] OSC's investigative functions can be triggered either by a tip from the public or federal employee, or independently by OSC upon identification of evidence indicating a potential violation of the Act.[51] To begin an investigation

---

39. *See* Hargreaves, *supra* note 9.

40. *Id.* at 227 (citing 5 U.S.C. §1215).

41. *Id.*

42. *See* JON O. SHIMABUKURO & JENNIFER A. STAMAN, CONG. RSCH. SERV., MERIT SYSTEMS PROTECTION BOARD (MSPB): A LEGAL OVERVIEW (2019); U.S. MERIT SYS. PROT. BD., AN INTRODUCTION TO THE MERIT SYSTEMS PROTECTION BOARD 4 (2007).

43. Shimabukuro & Staman, *supra* note 42 (noting that the "term of office for each Board member is seven years, and terms are nonrenewable.").

44. *See* U.S. OFF. OF SPECIAL COUNS., SPECIAL COUNSEL DELLINGER ANNOUNCES UPDATES TO OSC'S HATCH ACT ENFORCEMENT (2024). As of the writing of this note, this guidance has not been rescinded by the Trump Administration.

45. *Id.*

46. *See* Hampton Dellinger, *Time to Close the Hatch Act's Escape* Hatch, POLITICO (May 20, 2024), https://www.politico.com/news/magazine/2024/05/20/office-of-special-counsel-updating-rules-for-white-house-officials-00158687 [https://perma.cc/CD3L-PTXG].

47. *See id.*

48. Novak, *supra* note 16.

49. *Id.*

50. 5 U.S.C. § 1216 (a)(1), (2).

51. *See* U.S. OFF. OF SPECIAL COUNS., THE ROLE OF THE U.S. OFFICE OF SPECIAL COUNSEL 4 (2006);

from a tip, OSC requires a member of the public or another employee to fill out an online form with sufficient information.[52] During the ensuing investigation, OSC obtains relevant documents, conducts interviews,[53] and works alongside the subject's employing agency.[54]

If the Office of Special Counsel finds that the subject violated the Hatch Act but that the violation is not "sufficiently egregious to warrant prosecution," OSC will issue a warning letter to the subject of the investigation.[55] If, however, OSC's investigation leads them to believe that the violation requires disciplinary action, it can either move for a settlement or file a case with the Merit Systems Protection Board.[56] The majority of the time, cases are settled.[57]

If OSC chooses to file with the Board, it furnishes the Board and the subject of the investigation with a complaint and statement of facts.[58] In addition, the Office of Special Counsel recommends disciplinary measures to the Board, though the Board can and regularly does deviate from these recommendations.[59] 5 U.S.C. § 1215 lays out the procedural requirements for Merit Systems Protection Board adjudication[60] and provides protections for the subjects of investigations.[61] Board decisions can be appealed directly to the United States Court of Appeals for the Federal Circuit.[62] MSPB penalties include reprimands, grade reductions, suspensions, removal from office, and fines[63] which are subject to annual adjustment.[64]

E. CONNECTION TO MODEL RULES OF PROFESSIONAL CONDUCT

While the Model Rules only constrain attorneys and the Hatch Act only applies to government employees, the two overlap in practice. Failure to comply with the Hatch Act implicates the *Model Rules of Professional Conduct,* specifically Rule 8.4 sections (c) and (e). Rule 8.4(c) instructs that it is professional misconduct for a lawyer to "engage in conduct involving dishonesty, fraud, deceit, or misrepresentation,"[65] while Rule 8.4(e) states it is professional misconduct for a lawyer to

---

U.S. OFF. OF SPECIAL COUNS., *How to File a Hatch Act Complaint,* https://osc.gov/Services/Pages/HatchAct-FileComplaint.aspx (Nov. 24, 2024, 12:30 PM) [https://perma.cc/6QVC-P2NM].

52. *See id.* (noting that information to include in the complaint includes the agency and position of the subject of the investigation as well as "names and contact information of potential witnesses.").

53. *See* U.S. OFF. OF SPECIAL COUNS., YOUR ROLE IN AN OSC INVESTIGATION (2018).

54. *See* Hargreaves, *supra* note 9, at 242.

55. *See* U.S. OFF. OF SPECIAL COUNS., *supra* note 51.

56. *See* Hargreaves, *supra* note 9, at 243.

57. *See* U.S. OFF. OF SPECIAL COUNSEL ANN. REP. (2023), at 29.

58. *See* Brown, *supra* note 20, at 3; 5 U.S.C. § 1215(a)(1).

59. Hargreaves, *supra* note 9, at 244.

60. *See* 5 U.S.C. § 1215.

61. *Id.* These procedural protections include the right to discovery, representation, a hearing either before the Board or an administrative law judge appointed by the Board, and a written decision by the Board and its rationale for reaching its conclusion.

62. *See* Hargreaves, *supra* note 9, at 243.

63. *See* 5 U.S.C. § 1215; 5 C.F.R. § 1201.126(a).

64. *See* U.S. OFF. OF SPECIAL COUNS., *supra* note 10.

65. MODEL RULES R. 8.4(c).

"state or imply an ability to influence improperly a government agency or official or to achieve results by means that violate the Rules of Professional Conduct or other law."[66]

In its entirety, Model Rule 8.4 is designed to maintain the integrity of the legal profession.[67] Similarly, the Hatch Act aims to maintain the integrity of the civil service by ensuring federal employees maintain strict ethical standards on the job. In practice, the Hatch Act accomplishes this goal by preventing employees from engaging in partisan political activities while on the job or from utilizing their official titles in a political capacity to exert improper influence.[68] When an employee utilizes their official title during partisan activities, including posting on social media with their title in their profile, they run the risk of implying the government's endorsement. This would constitute a misrepresentation of a government agency's officially neutral position in partisan activities, which Model Rule 8.4(c) aims to prevent.

The same rationale connects the purpose of the Hatch Act to Model Rule 8.4(e). By preventing lawyers from asserting improper influence over officials or agencies, Rule 8.4(e) emphasizes the importance of public trust in the government. Likewise, the Hatch Act aims to prevent government officials from putting themselves in positions where they could exert improper influence by preventing employees from using their titles or official roles in partisan activities. In effect, the Hatch Act helps to prevent government attorneys from unwittingly violating Rule 8.4(e) by limiting an employee's ability to purport themselves as individuals that could influence agency decisions for partisan ends.

Rules 8.4(c) and (e) offer avenues to solve a problem associated with increased Hatch Act enforcement from AI—increased investigations from inadvertent or minor infractions of the Hatch Act's political speech prohibitions. If an infraction is minor or inadvertent, Rule 8.4(c) guides a government attorney to mindfully and honestly explain the infraction. Even with a potential increase in claims and investigations, 8.4(c) deters lawyers from engaging in dishonest practices with investigators.

Similarly, a lawyer may not run afoul of Rule 8.4(e) unless they leverage their government role in an improper manner. A government attorney would only be subject to Hatch Act enforcement should AI detect the attorney campaigned while on duty, but OSC concluded that the attorney did not leverage their government role improperly. Rule 8.4(e) thus limits ethics sanctions to more serious abuses of authority.

---

66. MODEL RULES R. 8.4(e).

67. *See* MODEL RULES R. 8.4 cmt.

68. *See* Brown, *supra* note 20 (describing in the "summary" section the purpose of the Hatch Act and how it allows for employees to engage in political activities "in their free time" and away from their workplace).

II. ARTIFICIAL INTELLIGENCE IN THE WORKPLACE AND GOVERNMENT

A. KEYSTROKE SURVEILLANCE SOFTWARE

AI surveillance software is uniquely suited to monitor employee behaviors in unprecedented ways. AI workplace technologies can be "best understood as computer systems and algorithms [used] 'to perform tasks that typically require human-level intelligence to optimize aspects of the workplace, including enhancing productivity, streamlining operations, and improving decision making.'"[69] AI surveillance can operate constantly and comprehensively,[70] unlike traditional methods of surveillance which may have required manual oversight from managers. The incentives for employers to adopt tracking software are amplified by the rise in work-from-home arrangements following the COVID-19 pandemic, since teleworking employers are unable to monitor employees in ways they would otherwise be able to in a physical office.

Certain workplaces are already taking advantage of this new technology.[71] As of 2023, "studies show that around 80% of large employers are using some type of monitoring software in the workplace."[72] Employers are increasingly adopting AI-powered tools to monitor productivity, ensure compliance with company policies, and prevent risks, including data breaches and malicious activities.[73] Some employers have even deployed software to "keep[] tabs on bathroom breaks."[74]

Productivity monitoring tools are utilized by employers to track employee productivity metrics. These can "identify the words that employees type, the websites they visit, the number of emails they send, and the number of steps or breaks they take."[75] Keystroke software, a specific kind of productivity monitoring tool, might prove particularly troublesome in the context of Hatch Act enforcement. Current keystroke software could be utilized with such a degree of specificity as to "identify workers' use of particular words or phrases."[76] Particular words and

---

69. Bradford J. Kelley, *All Along the New Watchtower: Artificial Intelligence, Workplace Monitoring, Automation, and the National Labor Relations Act*, 107 MARQ. L. REV. 195, 202 (2023) (quoting Bradford J. Kelley, *Wage Against the Machine: Artificial Intelligence and the Fair Labor Standards Act*, 34 STAN. L. & POL'Y REV. 261, 268 (2023)).

70. *See* Steven Greenhouse, *'Constantly Monitored': The Pushback Against AI Surveillance at Work*, THE GUARDIAN (Jan. 7, 2024), https://www.theguardian.com/technology/2024/jan/07/artificial-intelligence-surveillance-workers [https://perma.cc/C27M-BJ2M].

71. *See, e.g.*, Justin Doubleday, *With 'Spying Bosses' on the Rise, Where do Federal Agencies Stand on Employee Monitoring?*, FED. NEWS NETWORK (Apr. 8, 2024), https://federalnewsnetwork.com/federal-report/2024/04/with-spying-bosses-on-the-rise-where-do-federal-agencies-stand-on-employee-monitoring/ [https://perma.cc/WU35-QXRD] (illustrating "at least one instance" where the federal government has monitored remote employees for performance by surveying employee computer logs and phone records).

72. Kelley, *supra* note 69, at 203.

73. *See* Benjamin Wong, *Data Protection Implications of Modern Employee Monitoring Software*, 33 SINGAP. ACAD. L.J. 101, 102 (2021).

74. Greenhouse, *supra* note 70.

75. Kelley, *supra* note 69, at 196–97.

76. *Id.* at 199.

phrases, in the context of Hatch Act enforcement, could include candidates' names, political party affiliations, voting, or other partisan terms. In general, keystroke software is used by employers to ensure compliance with corporate policies.

B. KEYSTROKE SOFTWARE AS EMPLOYED BY THE GOVERNMENT

The government employs keystroke software, though whether it is used in detecting Hatch Act violations is unclear. Take, for instance, the Department of Veterans Affairs' (VA) use of InterGuard. First introduced into the Department in 2019, InterGuard was adopted to ensure that department personnel utilize government equipment for official business, preventing data loss and increasing productivity.[77] The VA website describes InterGuard as an "employee monitoring, web content filtering, keystroke logging, data loss prevention and laptop theft recovery software" with the power to comprehensively record an employee's computer activity to "ensure[] that personnel are utilizing government equipment for official business."[78]

InterGuard's keystroke tool allows Department officials to review employee keystrokes in any application.[79] Applications that track keystrokes include "web browsers, chats, Microsoft Office files, emails," and more.[80] Risky keywords, presumably set by the employer, are immediately flagged for supervisor attention.[81] Perhaps most striking is the fact that InterGuard logs all keystrokes for future audits, meaning that employers at the Department can, after time has passed,[82] review what employees have typed in the past. Users of InterGuard can also access the content of employees' email messages and attachments, including ones which have been deleted, as well as searches employees have made on computer hard drives.[83] The software can also monitor cell phone activity, including outgoing text messages, and internet activity.[84]

Widespread deployment of InterGuard or other keystroke software across the government would have a large impact on Hatch Act enforcement. Notably, InterGuard tracks keystrokes—not just searches. Imagine a federal employee accidentally types in a Google search, not realizing the phone they were using was their work device rather than their personal device. Even if the employee realized their error and deleted the text before clicking the search button, the

77. *InterGuard*, U.S. DEPT. OF VETERANS AFFS. (last visited Jan. 28, 2025), https://www.oit.va.gov/Services/TRM/ToolPage.aspx?tid=9456# [https://perma.cc/AV8X-TQD7].

78. *Id.*

79. *See Remote Employee Monitoring: The Quick Guide to Improving Productivity and Data Security*, INTERGUARD (last visited Jan. 28, 2025), https://www.interguardsoftware.com/remote-employee-monitoring/ [https://perma.cc/NN7T-EKGA] (explaining and listing the features of InterGuard. The InterGuard home page is linked from the Department of Veterans Affairs technical explanation of the software's adoption).

80. *Id.*

81. *Id.*

82. *Id.*

83. *Id.*

84. *Id.*

mere typing of the search terms could potentially trigger a warning from OSC. Their supervisor has seemingly unlimited access to audit the keystrokes and detect a potential violation, inadvertent though it may have been.[85]

This marks a fundamental change in Hatch Act detection. In the past, enforcement of the Hatch Act evolved as employees began actively utilizing mediums such as email or social media.[86] A supervisor's unlimited access to past messages and searches raises concerns about contextual misunderstandings—employees might jokingly reference politics in an email or instant message, discuss current events in a non-partisan manner, or even research a policy relevant to their job only for keystroke software to flag the action as a potential violation.

The government has an incentive to set many terms as "risky keywords" to maximize enforcement of the Hatch Act. As Special Counsel Dellinger put it, Congress "wants the Hatch Act to apply to as many people as possible."[87] Using keystroke software casts a wider net through its comprehensive surveillance at the risk of flagging innocent behavior. Even if the enforcement system is already overburdened, Congress wants broad application of the Hatch Act. As such, OSC has incentive to maximize coverage regardless of the strain, regardless of the impact on efficiency.

That is not to say that OSC would, or does, expect every flagged Hatch Act violation to result in a penalty. In determining penalties under the Hatch Act, the Merit Systems Protection Board looks to twelve factors, deemed the *Douglas* factors. Among others, the factors include "the nature and seriousness of the offense . . . including whether the offense was intentional or technical or inadvertent, or was committed maliciously or for gain, or was frequently repeated."[88] Even if MSPB is unlikely to assess penalties for typing in a "risky keyword" absent additional information—such as a history of violations by the employee at issue or clear intent to violate the Hatch Act—the Office of Special Counsel is still burdened by an increased number of potential violations. Investigating these potential violations take time and resources both from the Office of Special Counsel and the employee that is the subject of the investigation. While inadvertent or accidental keystrokes may not result in an official violation of the Hatch

85. The Hatch Act does not have a *mens rea* requirement, absent 5 U.S.C. § 7323(a)(2), (4), which prohibit employees from "knowingly" soliciting, accepting, or receiving a political contribution in certain cases and from discouraging those who have certain business pending before an agency from participation in political activity. Outside of these limited circumstances, more "typical" violations of the Hatch Act, including the provisions regarding employee participation in political activity, do not have a *mens rea* requirement.

86. *See* Brown, *supra* note 20, at 7.

87. *See* Dellinger, *supra* note 46.

88. U.S. MERIT SYS. PROT. BD., *Determining the Penalty* (last accessed Feb. 27, 2025) https://www.mspb.gov/studies/adverse_action_report/10_DeterminingthePenalty.htm#:~:text=The%20rules%20for%20determining%20the,to%20authorize%20the%20adverse%20action [https://perma.cc/S63G-NPHD]. Other factors include the employee's past disciplinary record, the notoriety of the offense or its impact upon the reputation of the agency, and the employee's past work records.

Act, they nonetheless raise the risk of triggering investigations and exacerbating the strain on the enforcement system.

The Office of Special Counsel does not comprehensively publish the total number of Hatch Act investigations conducted for a given year, but does provide some statistics on its enforcement actions. In its report to Congress for fiscal year 2024, OSC notes that it issued 967 advisory opinions and 81 warning letters.[89] In addition, OSC obtained 49 corrective actions through negotiated settlements "and seven disciplinary actions, either by negotiation or through MSPB order."[90]

While at first glance the raw data may suggest that OSC does not face a substantial burden, the Office sees it differently. Special Counsel Dellinger states that OSC received 6,251 total new cases in FY 2024, including Hatch Act claims, and claims of violations of other statutes that it is responsible for enforcing.[91] Dellinger notes that the number of cases is an increase of 45% over the prior five-year average. The rising number of cases "threatens to increase the number of active cases that OSC carries over to the following fiscal year."[92] Dellinger anticipates that the Office of Special Counsel will require additional resources since its caseload is expected to continue to increase—even before AI-powered software is added to the mix.[93]

C. FACIAL RECOGNITION SOFTWARE

Employers also use facial recognition and biometric technology to monitor employee productivity, track facial expressions and even register emotional responses. Facial recognition software can "grant[] the employer access to an employee's camera . . . to monitor when the employee is present."[94] Advanced software can even go a step further.[95] Employers have faced backlash for the intrusiveness and comprehensiveness of the technology.[96] One such employer, Pricewaterhouse Coopers (commonly known as PWC), has worked on developing a tool to "use[] employees' webcams to log absences from their desks."[97] Employees are then forced to provide written explanations for time spent away from their desks.[98]

---

89. U.S. OFF. OF SPECIAL COUNS, *Performance and Accountability Report for Fiscal Year 2024* 19 (2024).

90. *Id.*

91. *Id.* at 5.

92. *Id.*

93. *See id.*

94. Stephanie Creed & Alison Dixon, *Facial Recognition Technology in Employment: What You Need to Know*, BIRD & BIRD (Nov. 6, 2020), https://www.twobirds.com/en/insights/2020/global/facial-recognition-technology-in-employment [https://perma.cc/Q85P-J2A4].

95. Some systems employed in Chinese schools can even detect signs of engagement through facial expressions and then report these findings to teachers. *See* Nila Bala, *The Danger of Facial Recognition in Our Children's Classrooms*, 18 DUKE L. & TECH. REV. 249, 249 (2019-2020).

96. *See* Creed & Dixon, *supra* note 94; *see also* Ashleigh Webber, *PwC Facial Recognition Tool Criticised for Home Working Privacy Violation*, PERSONNEL TODAY (June 16, 2020) https://www.personneltoday.com/hr/pwc-facial-recognition-tool-criticised-for-home-working-privacy-invasion/ [https://perma.cc/3MTM-QUPU].

97. Creed & Dixon, *supra* note 94.

98. *Id.*

Take Amazon, for instance. In 2023, Amazon started tracking their delivery drivers by using cameras that employed artificial intelligence and biometric feedback indicators.[99] These indicators make a noise or inform drivers of potential driving infractions, such as a driver going over the speed limit, getting cut off, or taking their eyes away from the road momentarily.[100] Data from these cameras was sent directly to Amazon for review by supervisors, even when the camera incorrectly reported a violation.[101] One driver reported that the camera flagged him for a safety violation after scratching his beard, with the behavior being reported as him possibly using a cell phone while driving.[102] To remove this "negative mark" that the AI system made against him, the employee disputed the violation.[103]

It does not appear that the federal government currently uses facial recognition software for productivity monitoring searches. Instead, the government primarily employs such software for security purposes, including controlling access to buildings or government devices such as smartphones.[104] If the government were to decide to implement tracking software akin to that used by Amazon, enforcement of the Hatch Act could become more difficult. The error-prone nature of this technology leads to false-positive claims, and a system where employees may have to affirmatively dispute alleged violations. Both will lead to backlogs in the system.

Much like Amazon's delivery drivers, federal employees could find themselves under the eye of AI-powered cameras in the workplace for the purported goals of enhancing security effectiveness and efficiency. Again, though the federal government has not yet utilized such technology to monitor employee efficiency, it has begun large scale deployment of facial recognition software for other purposes.[105] More problematic for Hatch Act enforcement is the error-prone nature of these technologies. Just as an Amazon driver was reported for merely scratching his beard, federal workers could too face similar problems if, for instance, camera software mistakenly detected that items in the background of an employee's video call contained political material. The method by which Amazon drivers are required to address these erroneous claims also portends

---

99. *See* Cater & Heikkilä, *supra* note 6.

100. *See id.*; Lauren K. Gurley, *Amazon's AI Cameras are Punishing Drivers for Mistakes They Didn't* Make, VICE (Sept. 20, 2021), https://www.vice.com/en/article/amazons-ai-cameras-are-punishing-drivers-for-mistakes-they-didnt-make/ [https://perma.cc/HB65-89M2].

101. *See* Gurley, *supra* note 100.

102. *AI Tech Monitors Amazon Delivery Drivers*, KANE & SILVERMAN P.C. (last visited Jan. 28, 2025), https://www.palegaladvice.com/blog/ai-tech-monitors-amazon-delivery-drivers/ [perma.cc/S36M-ZL3U].

103. *Id.*

104. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-526, *Facial Recognition Technology: Current and Planned Uses by Federal Agencies* (2021).

105. *See Facial Recognition Technology*, TRANSP. SEC. ADMIN. (last visited Jan. 28, 2025), https://www.tsa.gov/news/press/factsheets/facial-recognition-technology [perma.cc/EQ85-FUQR]. Though the Transportation Security Administration does not currently use this technology for employee productivity monitoring, it has already begun rolling out facial recognition software at their flight security screenings for security and efficiency purposes—illustrating the government's capability of rolling out this sort of technology on a large scale.

stress on the Hatch Act systems. Should AI detect a potential Hatch Act violation, federal employees, like Amazon drivers, may have to affirmatively dispute each claim, creating an overload of falsely flagged violations that require some process to rectify.

The Fourth Amendment protects individuals against unreasonable searches and seizures,[106] and it is likely that government employees would have concerns with the amount of personal data their employing agency would be able to collect using keystroke and facial recognition software. Whether federal employees have a "reasonable expectation of privacy" under the Fourth Amendment, however, is context specific.[107] Courts have held that an employee's expectation of privacy may be reduced by prior notice, including a policy that the workplace is subject to search.[108] Many federal agencies explicitly notify employees of such policies which implicate government-issued phones, computers, and other devices.[109] While courts have not directly addressed the intersection of AI-powered facial recognition software and the privacy rights of federal employees, it stands to reason that courts may grant the government a wide berth should they make such policies clear to their employees.

III. IMPACT OF AI SURVEILLANCE ON THE HATCH ACT ENFORCEMENT SYSTEM

The use of both keystroke and facial recognition software powered by AI could significantly increase the number of potential Hatch Act violations that could be reported to the Office of Special Counsel. Should such a surge in reported violations occur, the Hatch Act Enforcement system will experience strain from an increase in the number of claims and the corresponding investigations and potential enforcement proceedings. While some of these claims may be based on purely innocent actions, the sheer increase in the volume of claims will invariably result in more work for the Office of Special Counsel.

The impact of AI surveillance on the Hatch Act enforcement system is less relevant in the context of Senate-confirmed employees who are not subject to MSPB enforcement mechanism. These employees might feel some consequences of AI surveillance insofar as more whistleblower claims could be brought to OSC, but they likely will not experience the impacts of a potential backlog in adjudication by MSPB since it is ultimately up to the President to determine disciplinary consequences for those claims.[110] It is arguably unlikely that OSC would receive more claims for Hatch Act violations by Senate-confirmed employees than they currently do. Senate-confirmed employees are more public facing in their political roles, and their

106. U.S. CONST. amend. IV.

107. *See* City of Ontario, Cal. v. Quon, 560 U.S. 746, 757–67 (2010) (holding that an assessment of whether government employees have a reasonable expectation of privacy must be addressed on a "case-by-case basis.").

108. *See* Turiano v. City of Phoenix, 562 F. Supp. 3d 261, 274 (D. Ariz. 2022).

109. *See, e.g.*, U.S. GEN. SERVS. ADMIN., GSA *Telecommunications Policy* (Apr. 24, 2021).

110. *See* Hargreaves, *supra* note 9, at 227.

activities are more widely reported on.[111] The focus of AI's impact on Hatch Act enforcement should remain on non-Senate-confirmed employees, since their actions are currently under less observation from the public than their Senate-confirmed counterparts.

A. LESSONS FROM ANOTHER ENFORCEMENT SYSTEM UNDER STRAIN

Enforcement systems which have undergone significant technological advancements, making it easier to identify violations, have struggled to adapt accordingly. A case study of the Internal Revenue Service (IRS) and its use of big data provides insight into potential consequences for the increased visibility of violations that will inevitably result from the increased use of AI in detecting Hatch Act violations. Additionally, an analysis of the IRS' Return Review Program reveals the consequences of automated surveillance tools providing false positives or inaccurate results, which also gum up enforcement systems.

The IRS has long employed big data analytics to increase its efficiency and ability to detect tax fraud.[112] In 2009, the IRS developed the Return Review Program, which screens individual tax returns claiming refunds to detect fraud.[113] The Return Review Program uses "machine learning algorithms to 'score' returns on their likelihood to be fraudulent by uncovering patterns in data associated with fraud."[114] Once the Return Review Program selects a return as potentially fraudulent, the refund procedure is frozen and the return is assigned for treatment.[115] The IRS then manually reviews returns with suspicious characteristics.[116]

A few key aspects of the Return Review Program are particularly relevant to the discussion of the impact that increased claims of Hatch Act violations will have on the Office of Special Counsel. Across all of the IRS' fraud prevention methods, including the Return Review Program, the total false detection rate peaked at 62% in 2020 and dipped as low as 47% in 2022.[117] Once a report is flagged as fraudulent, "[t]he IRS presumes that returns [selected by the fraud detection programs] are fraudulent until the taxpayer completes" remediation

---

111. *See, e.g.*, U.S. OFF. OF SPECIAL COUNS., HA-22-000173, REPORT OF PROHIBITED POLITICAL ACTIVITY UNDER THE HATCH ACT (RACHAEL ROLLINS) (2023) (detailing OSC's investigation into Rachael Rollins, former U.S. Attorney for the District of Massachusetts and the conclusion reached by OSC that she violated the Hatch Act in part by attending a partisan fundraiser in her official capacity); U.S. OFF. OF SPECIAL COUNS., HA-24-0000104, REPORT OF PROHIBITED POLITICAL ACTIVITY UNDER THE HATCH ACT (CARLOS DEL TORO) (2024) (detailing OSC's investigation into Carlos Del Toro, Secretary of the Navy, and OSC's conclusion that Secretary Del Toro violated the Hatch Act as a result of comments he made on a news show).

112. *See* Steven Toscher & Daniel Kellerman, *The Impact of Big Data on IRS Civil and Criminal Tax Enforcement*, 42 L.A. LAW 14, 15 (July/Aug. 2019).

113. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-18-544, *Tax Fraud and Noncompliance: IRS Could Further Leverage the Return Review Program to Strengthen Tax Enforcement* 2 (2018).

114. Toscher & Kellerman, *supra* note 112, at 16.

115. *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 113, at 11.

116. *Id.*

117. *See* NAT'L TAXPAYER ADVOC., *Annual Report to Congress* 43 (2024).

steps, which is often a confusing process.[118] The Office of Special Counsel should be wary of the IRS' procedure should agencies contemplate utilizing keystroke or facial recognition software. As mentioned, issues with both kinds of software raise the risk of false or irrelevant claims being brought to the Office of Special Counsel's attention. OSC might likewise struggle to manage the volume of activities incorrectly flagged as potential Hatch Act violations. In addition, much like taxpayers incorrectly flagged by the IRS face a complex and confusing process to prove their compliance, so might federal employees—all of which burdens the Office of Special Counsel's investigatory capacity.

Another important point is that the Return Review Program's selection criteria factors in "the agency's capacity to review selected returns" and other factors "that weigh the cost and risk to the IRS."[119] This selection criteria reflects the agency's understanding that an excess of flagged violations could create an unsustainable workload—and more fundamentally it is an acknowledgement from the agency that they do not have the capacity to review each potential violation by hand. The IRS expects to receive over one hundred million individual tax returns for tax year 2024,[120] a number that's admittedly much higher than the number of Hatch Act tips that OSC receives. Nonetheless, OSC and MSPB should take heed of the IRS' situation after the deluge of claims accompanying the use of big data should the government seek to use AI technology to flag Hatch Act violations.

Given that utilizing keystroke and facial recognition software introduces a higher degree of scrutiny over employee actions, the Office of Special Counsel and Merit Systems Protection Board will likely face a higher volume of questionable activities—false positives or not. This is especially important, given that OSC currently does not have an automated system to review claims. As a result, OSC and MSPB would likely have to institute procedures like the IRS to gauge OSC's capacity to investigate claims and MSPB's ability to adjudicate if necessary. Even if AI-powered systems would bring the Office of Special Counsel a greater number of actual Hatch Act violations, the overall influx of claims might result in the Office being more selective in terms of which claims it investigates.

CONCLUSION

The rise of AI-powered surveillance software, such as keystroke and facial recognition technology, threatens to overburden the Hatch Act enforcement system if adopted by the federal government to ensure employee compliance. Compliance with the Hatch Act implicates both Rule 8.4(c) and (e) of the *Model Rules of Professional Conduct* insofar as both seek to maintain the integrity of

118. *Id.* at 42

119. *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 113, at 9.

120. *See IRS Announces Jan. 27 Start to 2025 Tax Filing Season; Agency Continues Historic Improvements to Expand, Enhance Tools and Filing Options to Help Taxpayers,* INTERNAL REVENUE SERV. (Jan. 10, 2025) ("The IRS expects more than 140 million individual tax returns for tax year 2024 to be filed ahead of the Tuesday, April 15 federal deadline."). OSC does not publish the number of tips it receives.

the legal profession and preserve public trust in government by preventing lawyers from asserting improper influence from their positions.[121]

AI-powered surveillance poses new challenges for the Office of Special Counsel. Rather than relying on employee tips or self-initiated investigation, automated surveillance software could inundate OSC with detected violations with no guarantee of accuracy. Take the Department of Veterans Affairs' use of InterGuard which tracks searches, messages, and even keystrokes of "risky keywords." The pervasiveness of this surveillance could spike reports of accidental violations.

The federal government has not yet used facial recognition software for productivity monitoring or compliance, but private-sector examples such as Amazon's AI cameras in their delivery trucks reveal the risks and burdens of incorrectly flagging benign behavior. Similarly, the Internal Revenue Services' Return Review Program uses big data analytics for fraud detection and struggles with high rates of false positives. Subsequent manual review by staff burdens resources and creates a risk of inconsistent enforcement.

OSC and MSPB must approach AI-powered surveillance cautiously. Though the constant nature of their surveillance in theory could lead to enhanced compliance, they risk inundating the enforcement mechanism with higher volumes of potentially frivolous claims.

121. MODEL RULES R. 8.4(c); MODEL RULES R. 8.4(e).