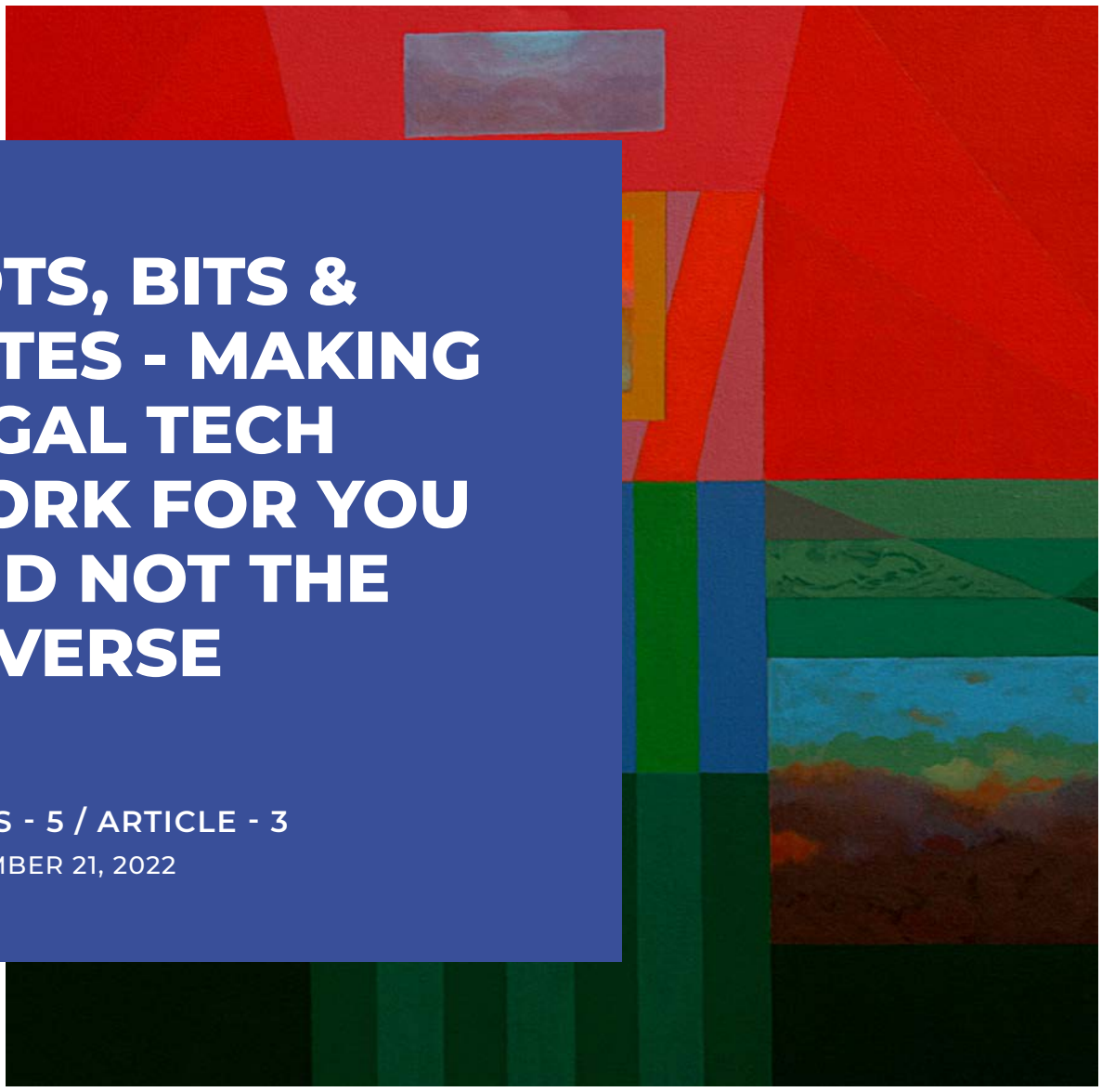
EMPLOYER TRACKING OF EMPLOYEE DATA



BOTS, BITS & BYTES - MAKING LEGAL TECH WORK FOR YOU AND NOT THE REVERSE

SERIES - 5 / ARTICLE - 3

SEPTEMBER 21, 2022

By **Jeffrey Brochin, Esq.**

GreenPoint> Law&Compliance

william.anderson@greenpointglobal.com | pranav.menon@greenpointglobal.com

International Corporate Center, 555 Theodore Fremd Avenue, Suite A102 Rye, NY 10580

www.greenpointlegal.com

Can your employer monitor your browsing history and other personal data of yours? The simple answer is—yes. And such employer tracking is becoming much more widespread in the era of Covid-19 remote work arrangements, with a plethora of tools available for use by your employer. We will examine how far your employer can go with such monitoring and the legal ramifications of overstepping those bounds.

Your 'Working' Assumption

Whether working from the office or home, your assumption should always be that your employer is monitoring you. Everything from your keystrokes to your browsing history and how much time you spend on which sites is all revealed. If you are connected to the internet via your employer's network, your employer has the right to track your internet activity; and, even if you are not connected to the company network, but are using company-issue equipment, the same employer rights apply. However, the laws get a bit murkier for the remote worker who is connected via a home network while using personal equipment.

What Might Get Tracked?

Some businesses have software installed, either on the company computer or via the company network that you access—even from home—that transmits copies of any emails sent to or from employee accounts, and certain software applications allow your employer to peruse deleted emails or unsent drafts. As to cellphone use, the employer can monitor text messages on a company-owned cellphone but not on your personal cellphone unless connected to the company network. Although using your own mobile data plan to access the internet will not expose your cellular activity to perusal, once your personal cellphone is operated via the company's network, your cellular activity can indeed be monitored. Think twice before storing passwords on a company cellphone, as even those can be subject to access by your employer's IT department.

Messaging Platforms Particularly Vulnerable

Essentially, your employer can access anything that you enter on a company messaging platform, and aside from access by the IT department, HR also often times can monitor those platforms, even if your direct manager or supervisor is less likely to have unqualified authorization to do so. Will all communications be checked? As a practical matter, it is highly unlikely that any employer will waste management's time reading all of your messages, unless there is a specific cause to do so, such as instances of employee theft, compromise of intellectual property, or serious fraud as to time-keeping or expense account charges. However, the fact that an administrator or manager can do so should put you on notice that this particular platform is highly susceptible to employer tracking.

From a Legal Perspective

Almost every court to decide employer data tracking cases has ruled that the employer has the right to read emails that employees have sent using the employer's company email system, even if the employee intended such messages to be private or confidential. To avoid litigation over such matters, many employers will fully disclose their practices and capabilities upfront and have employees sign an acknowledgment or waiver regarding the company's practices. However, even in the absence of such employee consent, courts have ruled that employers have extensive freedom to monitor the use of their own email systems.

Regarding personal email accounts, the law is less clear: some courts have held that employers may monitor an employee's personal email if the employee is using the company's equipment and the employee has been given notice that company-issued equipment is not for personal use. But such rulings are not universal, and variations exist from one jurisdiction to another, as do the fact-specific circumstances of each case.

Employer Rights Under the ECPA

Under the federal Electronic Communications Privacy Act of 1986 (ECPA), employers must demonstrate that they have a legitimate business reason for tracking employee data. While the ECPA contains provisions protecting employee privacy rights, at the same time, it recognizes that there exist legitimate reasons for accessing data created by or exchanged by employees. The Act defines 'electronic communications' as any electronic messages currently being transmitted, however, after transmittal, such messages are categorized as 'electronic storage', and are then governed by the Stored Communications Act.

Furthermore, under the ECPA's 'consent exception', much broader monitoring by employers is permitted, as noted above. The ECPA's 'business use exception' provision further expands monitoring of electronic communication of employees when legitimate business reasons to do so exist.

As the COVID-19 pandemic continues to shift more work to a remote-work model, the need for employers to maintain basic monitoring of employee productivity levels while operating within legitimate privacy limitations will need to be carefully balanced. Greater guidance will assist employers as the law progresses in this area. But in the meantime, both employers and employees will have to openly carve out what employer tracking will mean at any particular business.

Executive Summary

1. The Issue

Where does employer tracking of employee data stand in both the remote-work and in-office environments?

2. The Gravamen

Employers enjoy such widespread rights to monitor employee data, that all employees should assume that nothing they communicate over an employer network or at home via employer equipment, is private.

3. The Path Forward

Employees would be wise to strictly limit any private content they do not want exposed, and employers should craft full disclosure documentation to avoid unwanted legal entanglements.

Action Items:

1 Review:

Conduct a survey of your company's employee monitoring policies to make sure they comply with federal and applicable state regulations.

2 Draft:

Once a compliance review has been completed, reduce your company's monitoring policy to a written document with the assistance of IT, HR, and legal counsel.

3 Authorizations:

Define who will have access to employee data and for what purposes, in order to avoid illegal intrusions, and have in place a monitoring authorization procedure.

4 Disclose:

Be transparent with employees as to exactly what the company policy is regarding employer monitoring of data, whether communicated via company network or off-site company equipment.

Further Readings

1. https://www.morningbrew.com/hr/stories/2022/01/19/employee-surveillance-is-exploding-with-remote-work-and-could-be-the-new-norm
2. https://www.brookings.edu/blog/techtank/2021/01/05/how-employers-use-technology-to-surveil-employees/
3. https://nanoglobals.com/can-boss-see-my-browsing-history/
4. https://www.businessnewsdaily.com/6685-employee-monitoring-privacy.html
5. https://www.currentware.com/blog/workplace-privacy-employee-monitoring/

Jeffrey Brochin, Esq.

GREENPOINT STAFF COUNSEL
AND CONTENT EDITOR

After receiving his Juris Doctor degree from The John Marshall Law School in Chicago, Mr. Brochin served as an Administrative Law Judge with the Illinois Department of Labor for six years where he presided over cases dealing with job separation issues and matters pertaining to contested Unemployment Insurance claims. He also co-wrote the agency's administrative rules, and periodically served as a 'ghost writer' for Board of Review decisions. Following that position, he was Director of Development for a Chicago-area non-profit college where he was responsible for High Net Worth donations to the institution. For the next eighteen years he practiced as a solo practitioner attorney with an emphasis in the fields of Real Estate law and Commercial Contracts transactions, and was an agent for several national title insurance agencies.

In 2003 he was recruited to head up a U.S. title insurance research office in Israel, a position he held for four years, and between 2007-2017 he participated in litigation support for several high-profile cases. He has taught Business Law as a faculty member of the Jerusalem College of Technology, and has authored a wide variety of legal White Papers and timely legal articles as a professional legal content writer for GPL clients. Separate from his legal writing, he has co-authored academic articles on Middle East security topics that have been published in peer-reviewed publications.

William H. Anderson, Esq.

MANAGING DIRECTOR AND HEAD OF
FINANCIAL PRODUCTS AND SERVICES

William Anderson is Managing Director and Head of Law & Compliance. He leads the GreenPoint practice in providing regulatory, legal, and technology solutions to law firms, legal publishers, and in-house law departments around the world, overseeing our team of experienced US attorneys and data and technology experts. Will has over 25 years' experience working with corporations to improve the management of their legal and corporate compliance functions. Will began his legal career as a litigator with a predecessor firm to Drinker, Biddle LLP. He then served as in-house counsel to Andersen Consulting LLP, managing risk and working with outside counsel on active litigation involving the firm.

Will has leveraged his legal experience interpreting regulations and appearing before federal (DOJ, SEC, FTC) and state agencies (NYAG) to oversee research and other areas at Bear Stearns. In this capacity, he counseled analysts on regulatory risk and evolving compliance requirements. Will also consulted on the development of a proprietary tool to ensure effective documentation of compliance clearance of research reports. Will then went on to work in product development and content creation for a global online compliance development firm pioneering the dynamic updating of regulated firms' policies and procedures from online updates and resources. Will holds a Juris Doctorate with High Honors from the Washington University School of Law in Saint Louis and is admitted to state and federal bars. He lives in Pawling, NY, with his wife and daughter.

Sanjay Sharma, PhD

FOUNDER AND CHAIRMAN

Pranav Menon, Esq.

LEGAL RECRUITMENT
MANAGER AND DATA
PRIVACY SPECIALIST – LAW
& COMPLIANCE | GPESR

GreenPoint> Law&Compliance

About GreenPoint Law & Compliance

- GreenPoint Global was founded in 2001 and since that time has faithfully served an expanding roster of clients. GreenPoint leverages a unique combination of US-trained attorneys and proprietary technology to deliver a unique offering of skill and flexibility to meet client needs.
- Our core team of experienced US attorneys is based in Israel and works US hours. The breadth of experience of our attorneys ensures high-quality, cost-effective results across a wide range of legal, compliance, and regulatory matters.
- GreenPoint's methodology and proven track record of achieving client objectives has resulted in a broad base of clients in the United States, ranging from Fortune 500 insurance companies to solo practitioners, law firms, in-house law departments, and legal publishers. GreenPoint attorneys are selectively recruited and deployed based on possessing demonstrable subject matter expertise covering a broad spectrum of substantive US laws and regulations. The work product of our attorneys is thoroughly vetted internally before delivery to client. Adherence to quality, value and flexibility is at the core of our foundation.

GreenPoint> Global

About GreenPoint Global

- GreenPoint Global provides litigation support, finance and technology solutions to insurers, law firms, banks, and in-house law departments through our subject matter experts and process specialists.
- Founded in 2001 and headquartered in Rye, New York, GreenPoint has grown to over 500 employees with a global footprint. We have a stable and growing client base that ranges from small and medium-sized organizations to Fortune 1000 companies worldwide. Our production and management teams are located in the US, India, and Israel with access to deep pools of subject matter experts. Our greatest strength is our employee-base of experienced lawyers, paralegals, process specialists, financial analysts, and software developers. We have leading edge software development capabilities with over 50 professionals on staff, working on internal and client projects.
- GreenPoint is certified by the TÜV SÜD (South Asia) for the highest standards of Quality Management (ISO 9001:2015) and Information Security Management (ISO 27001:2013). GreenPoint is certified as a Minority and Woman Owned Business Enterprise (MWBE) by New York City and a Minority Owned Business Enterprise (MBE) by the State of New York. GreenPoint complies with all federal and state contracting requirements. GreenPoint is owned by its founders and principals and is debt free. For comprehensive information on our services and products under Law & Compliance and Finance, please visit our subsidiary websites through the division's menu.