THE ROLE OF GPS AND CELL PHONE TRACKING OF EMPLOYEES IN BIG DATA LAW

Joanna P. Kimbell[*]

In *GPS and Cell Phone Tracking of Employees*,[1] Professor Marc McAllister makes a case for limiting the use of cell phone tracking of employees to either noninvestigatory, work-related purposes or misconduct investigations wherein the use of tracking is used only as a means to corroborate evidence that the tracked employee has committed a terminable offense. As Professor McAllister notes, disgruntled employees subject to tracking by employers may seek to sue for invasion of privacy.[2] Professor McAllister offers guidance to employers for four different employee tracking scenarios to defend against such suits. By focusing attention on the legal issues around tracking, Professor McAllister has added to the body of Big Data legal scholarship, illuminating one zone of the greater sphere. His focus on legal issues from the employer's perspective invites comment and analysis from the view of the employee and reflection on individual data privacy more generally.

I. PROFESSOR MCALLISTER'S ANALYSIS

Professor McAllister separates his analysis into GPS tracking and cell phone tracking. He further separates the analysis into noninvestigatory, work-related purposes tracking and misconduct investigation tracking. The first division is a recognition that while GPS tracking has some developed case law and precedents, the law for cell phone tracking is still evolving. Through the second division, Professor McAllister highlights an important legal distinction in employer tracking law: The purpose of the tracking determines the direction of legal analysis. Additionally, Professor McAllister notes there is a difference in analysis for public employers versus private employers, the lawfulness of tracking by the former dependent on the Fourth Amendment to the United States Constitution and the latter on tort law.[3] Professor McAllister's analysis and notes regarding the history of Fourth Amendment law in this area,[4] would well serve 1L students learning about search and seizure and its application to employment law as it adroitly summarizes the more established points of law. Beyond that, Professor McAllister makes a new contribution to the field of data privacy in his delineation of existing law for GPS tracking and recommendations related to cell phone tracking.

---

* Clinical Assistant Professor of Business Law & Management, West Texas A&M University.

1. Marc Chase McAllister, *GPS and Cell Phone Tracking of Employees*, 70 FLA. L. REV. 1265 (2018).

2. *Id.* at 1317.

3. *See id.* at Parts I.A., I.B.

4. *See id.* at 1269–79 nn.21–98.

According to Professor McAllister's analysis, to ensure that employers may use GPS tracking for both noninvestigatory, work-related purposes and misconduct investigations that may result in disciplinary actions, there should be an employee consent to tracking,[5] a legitimate business purpose necessitating the use of GPS,[6] and a limitation by the employer on data collection—specifically, a decision to not collect GPS data while employees are off duty.[7] GPS tracking can be used for misconduct investigations, but "employers should utilize this highly intrusive investigative technique only as a last resort, and only insofar as is truly necessary to corroborate an allegation of serious misconduct."[8]

Interestingly, Professor McAllister affords cell phone tracking some different treatment than GPS tracking, focusing more on notice and consent. The difference reflects how cell phone tracking methods by law enforcement are treated by the courts, specifically, how the location of a cell phone can be tracked without a physical trespass being committed on the cell phone, unlike when law enforcement attaches a GPS tracking device to a vehicle.[9] Professor McAllister notes that because there is no physical trespass to track the location of a cellphone, such an investigatory method will generally be subject to fewer constitutional constraints than GPS tracking.[10] Employers will most likely track employees through smartphone apps.[11] Whether collecting information about an employee's location using such apps can trigger Fourth Amendment protection depends on the employee's ability to demonstrate a reasonable expectation of privacy.[12] As noted by Professor McAllister, the expectation of privacy under such circumstances generally depends on whether the employee had notice of the monitoring and consented to it.[13] Presumably, the employee had notice when the employer stated that downloading and using the app were job requirements.[14] Professor McAllister notes that the notice and consent requirement is normally part of the expectation of privacy in the employment context,[15] but it is not clear that notice and consent will be the default standard within the employment context for cell phone tracking misconduct investigations by

5. *See id.* at 1309.
6. *See id.*
7. *See id.* at 1303, 1309.
8. *Id.* at 1303.
9. *See id.* at 1310.
10. *Id.*
11. *Id.* at 1313–14.
12. *See id.* at 1291–92
13. *See id.* at 1308–09, 1315.
14. Form and sufficiency of such notice was not in the scope of Professor McAllister's article and as such will not be scrutinized here, though this author does note that such an issue is relevant generally in a broader analysis of individual protections in Big Data law.
15. *Id.* at 1315.

private employers. Rather, it may simply be a preexisting condition of using cell phone app-tracking methods.

Professor McAllister draws on a recent New York case, *Carniol v. N.Y.C. Taxi & Limousine Comm'n*,[16] as the base for his recommendations to employers using cell phone tracking for misconduct investigations.[17] However, the case involved GPS tracking, not cell phones and the tracking was conducted by the city of New York.[18] GPS data of taxi cabs was originally collected for administrative purposes,[19] purposes recognizable as noninvestigatory or work-related, and later used to conduct a misconduct investigation related to fares.[20] The New York Supreme Court focused on contextual issues to determine if a taxi driver, Robert Carniol, had a reasonable expectation of privacy, and determined that in a highly regulated industry like the taxicab industry, no such reasonable expectation existed.[21] This could be a point for a parallel argument to be made in a later cell phone tracking case, an argument that an employee having no ownership of the data generated by a tracking app on their phone has no reasonable expectation of privacy in the data. Professor McAllister does acknowledge this potential argument.[22] He also predicts that a misconduct investigation using cell phone tracking would be similar to *Carniol* because it would likely stem from an employer reviewing data previously collected on several employees for some noninvestigatory, work-related purpose.[23]

What Professor McAllister does not discuss in detail is the issue of notice and consent for cell phone tracking misconduct investigations. Are we to assume that the notice and consent that occurred at the outset when the employee agreed to the cell phone tracking for the noninvestigatory, work-related purpose carries over to a misconduct investigation, or should some additional or exceptional notice and consent be required?[24] After all, the reasonableness requirements for GPS tracking between noninvestigatory, work-related searches and misconduct investigations are different. If that difference is solely the result of the fact that in the latter investigation there is a physical trespass that occurs without consent, then notice and consent could be a common standard required for both types of cell phone tracking because there is no physical trespass

16. 975 N.Y.S.2d 842 (N.Y. Sup. Ct. 2013), *aff'd*, 2 N.Y.S.3d 337 (N.Y. App. Div. 2015).
17. McAllister, *supra* note 1, at 1316–17.
18. *Carniol*, 975 N.Y.S.2d at 844.
19. *Id.*
20. *Id.* at 845.
21. *Id.* at 848.
22. McAllister, *supra* note 1, at 1317.
23. *Id.*
24. One possible requirement is specific language in the notice or consent, which takes place between the employer and employee and states that the data can be collected and analyzed for purposes not limited to the original noninvestigatory, work-related purpose.

in either case. However, if more than physical trespass drives reasonableness requirements, then an argument could be made using the reasonable expectation of privacy test in *Katz v. United States*[25] to limit the use of data collected even where there is notice and consent.[26] Provided it can be shown that an employee's expectations of how data will be used are part of such reasonable expectation of privacy.[27] If court rulings take that position, we could see application of detailed outset and scope reasonableness requirements for cell phone tracking, as opposed to notice and consent. We could also see the idea that if the employer owns the generated data, then it is sufficient to nullify the employee's claims of reasonable expectation of privacy.[28]

What *Carniol* really achieves in terms of possible application to tracking through technology other than GPS, is confirmation that the determination of a reasonable expectation of privacy is contextual. Notice and consent at the outset is not an absolute standard for determining reasonable expectation of privacy; it is simply one contextual factor, and therefore should not be assumed to be the standard for cell phone tracking misconduct investigations.

II. BIG DATA LAW

Professor McAllister's paper may be classified among the growing body of Big Data legal research. Technology has changed the legal environment, and despite some early efforts to regulate free speech issues online, legal issues related to free speech and privacy are abound.[29] Many of these issues can be traced to, and some are directly driven by, Big Data.

Big Data is more than bits and bytes. It is vast quantities of data and the productive activities that use that data by harvesting, analyzing, and transforming it into viable information. As an information source, it can create value, but its collection and generation spawn numerous privacy

25. 389 U.S. 347 (1967).

26. *Id.* at 360–61 (Harlan, J., concurring) (identifying and discussing the reasonable expectation of privacy test).

27. Professor McAllister discusses the concurring opinions in *United States v. Jones*, 565 U.S. 400 (2012), and the *Katz* test relative to length of surveillance as being a defining factor in the scope of the surveillance. *See* McAllister, *supra* note 1, at 1292–93.

28. *See* McAllister, *supra* note 1, at 1303–04 nn.274–75 (discussing how expectations of privacy shift depending on who owns the property subject to intrusion, particularly when ownership is accompanied by notice and consent).

29. *See* Joanna P. Kimbell, *Turning a Blind Eye to Mob Justice: How 20-Year-old First Amendment Cases and Regulations Erode Internet Free Speech* 22–27 (S. Acad. of Legal Studies in Bus., Working Paper, 2019) (discussing the Communications Decency Act passed in 1996 and its current impact on free speech and anonymity on the internet).

concerns.[30] Big Data, in terms of its relevance to individuals, can be split into three categories: social, employment, and legal. Classification of a data set is determined by identifying the primary sphere of influence in which a second or third party's use of the data impacts an individual, who is the original generator or source of the data.[31] Employment data is data about an individual used by a potential or current employer and can be sub-categorized as pre-employment or employment data. Employment data, like the GPS data examined in this article, is data generated by the individual—the employee—after being hired and used by the employer for matters that impact the employee's continuing employment.

The most commonly known types of employer Big Data searches are pre-employment credit report searches and searches of employee internet activity and emails during employment.[32] By focusing on GPS data and cell phone searches by employers vis-à-vis apps, Professor McAllister expands the discussion of employer searches. While the tracking activities he discusses may be less known—and depending on the industry, less prevalent than employer searches focusing on employee email and internet use—the information and analysis are valuable for two reasons: First, they bring attention to GPS and cell phone tracking by employers; Second, they expand our understanding of individual rights and Big Data in the current legal environment.

Thus, Professor McAllister's analysis can be extended by taking the information from the employer-focused analysis and examining the same issues from the employee perspective. This allows us to compare such employer-driven searches with other searches impacting the rights of individual employees. According to Professor McAllister, the controlling law for GPS and cell phone tracking is tort law, which implements some aspects of the Fourth Amendment.[33] However, because the question of employee consent may impact some court decisions about whether the employee had a reasonable expectation of privacy, contract law also

30. *See* Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63, 63–65 (2012) (discussing the new views of data in the Big Data age, benefits of Big Data, and general privacy concerns about its collection and use).

31. The sphere of influence for data use may not be the same as the sphere of data generation, as when an individual uses social media for what is believed to be purely social reasons, but then a potential employer uses the socially generated data for a pre-employment screening.

32. *See* Ruth Desmond, Comment, *Consumer Credit Reports and Privacy in the Employment Context: The Fair Credit Reporting Act and the Equal Employment for All Act*, 44 U.S.F. L. REV. 907, 907 (2010) ("The use of credit reports in pre-employment background checks has become a prevalent practice among employers in recent years."); Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 48 AM. BUS. L.J. 285, 286 (2011) ("[T]he majority of employers monitor the electronic activities of their employees in some form or another.").

33. *See* McAllister, *supra* note 1, at 1279–80.

weighs heavily on the issue.[34] An employee's perspective—especially in the realm of Big Data, generally—is also of great interest as it raises the questions of the rights of the individual to privacy and the data generated. These same questions arise in relation to pre-employment checks. There too, the employee's agreement to allow collection, analysis, and use of the data by the employer is a condition of employment, the result at the pre-employment stage of a prospective employee refusing consent being the loss of the job opportunity.

Notably, the two kinds of searches are very different in another way. At present, there is no federal regulation governing how employers collect and use GPS or cell phone tracking data.[35] Pre-employment credit checks, however, are governed by the Fair Credit Reporting Act (FCRA).[36] The Act allows employers to perform credit checks but requires that prospective employees are given notice, a right to correct data, a right to appeal the results, and other remedies depending on the content of data in the report and the action taken by the prospective employer.[37] Notably, prospective employees have the right and the ability to access their data and see who has requested and viewed their credit information,[38] whereas with GPS or cell phone tracking employees do not know exactly what has been viewed or, in the case of misconduct investigations, for what purpose it was viewed.

As mentioned previously, Professor McAllister examines two different types of employer search scenarios: misconduct investigations and searches for noninvestigatory, work-related purposes. The latter is most likely to require employee consent, while there is no notice or consent requirement for GPS tracking in misconduct investigations. Comparing this to pre-employment Big Data searches, it is interesting to note that there is one noticeable example of searches for which there is no notice or consent: searches of online social networking searches for pre-employment. Employers use social networking platforms "as a simple and inexpensive way to perform background checks on

34. *Id.* at 1271 (noting that in "the employment context, expectations of privacy also largely depend on whether an employee has been notified of, and has consented to, the monitoring at issue"); *see id.* at 1275 (mentioning that the notice and consent requirement is one difference between the employment and law enforcement contexts); *id.* at 1271–72 (noting that courts' rulings on cases in the employment context also consider ownership of the property subject to intrusion); *id.* at 1270 (acknowledging that the aforementioned are in addition to other context-specific factors).

35. However, some states have statutes requiring consent for employer GPS tracking. *See id.* at 1280.

36. Pub. L. No. 91-508, 84 Stat. 1127 (1970).

37. *See* Kelly Gallagher, Note, *Rethinking the Fair Credit Reporting Act: When Requesting Credit Reports for Employment Purposes Goes Too Far*, 91 IOWA L. REV. 1593, 1602 (2006).

38. *See* 15 U.S.C. § 1681d(a)(1) (2012).

candidates" but do so without notice or consent.[39] Given the impact of notice and consent with some employment searches like GPS tracking, should the question of notice and consent in pre-employment searches be given more attention? Should all pre-employment uses of Big Data, regardless of the origination sphere of the data, be treated the same? Should all require notice and consent?[40] This is one example of how a paper like Professor McAllister's can stimulate analysis of other Big Data questions, and as questions about privacy and data rights continue to impact individuals socially and economically. Such analysis needs to continue.

Big Data law is in a challenging stage of development. Because it is still a young field, it may seem that the law is insubstantial. In fact, there is clear controlling law on some issues, and where there is not clear precedent on a particular fact pattern (like specific, new technology or new application), there may be sufficient information from related cases to outline best practices—as Professor McAllister has attempted to do by recommending legal guidelines for employers to conduct GPS and cell phone tracking searches. Still, with technology constantly changing, along with our awareness of the ways that use of technology and interactions in the online environment impacts our rights, research in this area is in a state of flux and comprehending it is more akin to tracking a light beam than grasping a tome. We must respect the nature of the task in our approach, seeing Big Data law as a prism to be held up to a light, each issue being examined and appreciated through various facets to be understood, with the lights and shadows cast being—in lieu of clear facts and specific precedents—the truest and clearest answers the field can currently produce.

---

39. Donald Carrington Davis, Note, *MySpace Isn't Your Space: Expanding the Fair Credit Reporting Act to Ensure Accountability and Fairness in Employer Searches of Online Social Networking Services*, 16 KAN. J.L. & PUB. POL'Y 237, 237 (2006).

40. For discussions of how the FCRA might be amended to extend protection to social media pre-employment screenings, see Nathan J. Ebnet, Note, *It Can Do More than Protect Your Credit Score: Regulating Social Media Pre-Employment Screening with the Fair Credit Reporting Act*, 97 MINN. L. REV. 306, 308 (2012) (noting that pre-employment screenings of social media by employers avoid FCRA restrictions when they are not conducted by third parties). *See also* Davis, *supra* note 39, at 237 (arguing that the FCRA should be amended to cover more pre-employment social media screenings).