BALANCING PRIVACY PROTECTIONS WITH ANTITRUST COMPLIANCE EFFORTS: KEY ISSUES AND POTENTIAL SOLUTIONS

BY FIONA SCHAEFFER, NATHANIEL MATTISON & JENNA WEINBLATT[1]

1 Fiona Schaeffer is a partner at Milbank LLP. Nathaniel Mattison and Jenna Weinblatt are associates at Milbank LLP.

Visit www.competitionpolicyinternational.com for access to these articles and more!

I. INTRODUCTION

Public interest in strengthening privacy protections and in pursuing more vigorous antitrust enforcement have increased in recent years, as certain economic sectors have been perceived to have become too consolidated and certain companies too powerful. Privacy and antitrust have the potential to be strong complements, in that they share the goal of protecting consumers from unfair economic exploitation – privacy law by promoting transparency in personal data collection and limiting the uses to which it may be put, antitrust law by promoting full and fair competition between providers of goods and services. Yet as legislatures move to strengthen privacy protections, broadly written statutes threaten to undercut effective antitrust compliance. Specifically, broad privacy protections may chill implementation of robust voluntary antitrust compliance programs if they limit employers' latitude to collect and analyze employee data necessary to carry out effective internal monitoring and timely report wrongdoing to enforcement authorities. Privacy is an important value, but legislators should take other policy goals into account when crafting new privacy protections: antitrust enforcers' increasing incentives for robust antitrust compliance programs also serve worthy social and economic purposes. Legislators, businesses, and the legal community should work together to ensure that privacy protections do not raise the risk of anticompetitive conduct going undetected, to consumers' detriment.

II. THE INCREASING PROMINENCE OF COMPLIANCE IN ANTITRUST ENFORCEMENT

A. The U.S. Department of Justice's Changing Approach to Compliance

For many years, antitrust enforcers in the United States treated corporate compliance programs with "disdain," as one commentator has put it.[2] Under the Corporate Leniency Program, only the first company to confess to participation in an antitrust crime and fully cooperate with the Department of Justice's Antitrust Division ("DOJ") could receive full recognition for its efforts — namely, immunity from prosecution. Companies that did not win the "race" for leniency had to plead guilty to criminal charges before having the opportunity to earn a reduction in the applicable penalties. A company's antitrust compliance program was only considered — if at all — as part of this sentencing reduction.[3] The DOJ took this stark approach to compliance and reporting because it was a tool to promote the Leniency Policy.[4]

2 Joseph E. Murphy, *Policies in Conflict: Undermining Corporate Self-Policing*, 69 Rutgers U.L. Rev. 421, 461 (2017).

3 Makan Delrahim, Assistant Att'y Gen., Antitrust Div., U.S. Dep't of Justice, Wind of Change: A New Model for Incentivizing Antitrust Compliance Programs, Remarks at the N.Y.U. School of Law Program on Corporate Compliance and Enforcement 2 (July 11, 2019), available at https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-new-york-university-school-l-0 ("Wind of Change").

4 *Id.* at 3.

Experience, however, seems to have taught the DOJ that a more sensitive — and sensible — approach to encouraging the development of compliance programs is required. Thus, in July 2019, Assistant Attorney General Makan Delrahim announced that the DOJ will begin considering whether to provide credit for businesses' compliance programs at the *charging* stage of criminal antitrust investigations,[5] and the DOJ has released public guidance for prosecutors — and companies — to assess companies' antitrust compliance efforts.[6] While the DOJ continues to disfavor non-prosecution agreements, except for those first-reporting companies that qualify under the Leniency Program, second- or third-to-report companies may now qualify for deferred prosecution agreements with federal prosecutors.[7] In this way, the DOJ is seeking to better leverage existing resources — and encouraging the new deployment of private ones — to eliminate anticompetitive behavior.

B. The Department of Justice's Guidance on Effective Compliance

To identify worthy compliance efforts, DOJ prosecutors now are to consider three core questions:

1. Is the corporation's compliance program well designed?
2. Is the program being applied earnestly and in good faith?
3. Does the corporation's compliance program work?[8]

The DOJ explicitly recognizes that "no compliance program can ever prevent all criminal activity by a corporation's employees,"[9] but companies nonetheless should strive to answer these questions satisfactorily, to mitigate the risks of criminal anticompetitive activity occurring and to earn credit with prosecutors as they weigh criminal charges. To make these broad questions more tangible, the DOJ helpfully has identified nine elements that commonly characterize effective antitrust compliance programs, which prosecutors are to consider when evaluating potential criminal charges:

1. Program comprehensiveness,
2. A corporate culture of compliance,
3. Senior management responsibility for compliance,
4. Risk assessment and appropriate program tailoring to a company's business,
5. Adequate training and communication,
6. Periodic reviews, monitoring and auditing,
7. Reporting mechanisms,
8. Incentives and discipline, and
9. Ongoing program improvement.[10]

---

5 *Id.* at 3, 6-9.

6 Antitrust Div., U.S. Dep't of Justice, Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations (July 2019), available at https://www.justice.gov/atr/page/file/1182001/download ("Evaluation of Corporate Compliance Programs").

7 Delrahim, Wind of Change, *supra* note 3, at 8.

8 DOJ, Evaluation of Corporate Compliance Programs, *supra* note 6, at 2.

9 *Id.* at 3.

10 *Id.* at 3-14.

While certain aspects of the DOJ's new approach will take time to work out — for example, establishing what might be sufficiently "prompt" reporting of wrongdoing for a company to merit a favorable charging decision — the DOJ's guidance is a clear signal to companies that antitrust compliance programs matter. Furthermore, while the guidance states that the nine markers of effective compliance are "not a checklist or formula,"[11] those markers provide a detailed and fairly straightforward roadmap for companies on how to establish promising compliance programs, and how to improve existing ones. Although the success of compliance programs can only be proven through experience, companies would be well served to invest in them: not only might they provide protection in the event of an investigation, they also point towards a better way of doing business.

III. STRENGTHENED PRIVACY LAWS: POTENTIAL BRAKES ON EFFECTIVE COMPLIANCE PROGRAMS

The DOJ's changed stance towards compliance programs, and specific guidance regarding the hallmarks of corporate good citizenship, are welcome developments for companies, practitioners, and consumers. Robust and widespread corporate self-policing is key to safeguarding the benefits of full and fair competition in markets. Trends towards strengthening privacy laws, however, may prevent companies and the DOJ from realizing the full potential of this changed approach, or seeing it copied by other jurisdictions.

A. The Traditional Rules of Privacy in the Workplace: Few Obstacles to Implementing Effective Compliance Programs

Historically, U.S. law has been favorable to employers' monitoring employees' use of company resources, such as workplace email, notwithstanding the potential presence of information employees might subjectively view as "private." Federal statutes regarding the interception of electronic communications, as well as the accessing of stored communications, contain exceptions for employers that allow them to review communications made using the employers' systems.[12] More generally, U.S. courts have applied a rule of an employee's reasonable expectations of privacy when deciding whether an employer's accessing an employee's data in the workplace — including on work-provided devices — is lawful.[13] Thus even information that an employee might argue is subject to his or her individual legal privilege may be accessed and used by an employer, if the employee objectively had no basis to believe that the information was not accessible or subject to monitoring or review.[14]

Friction around employer monitoring of employees has been building, however, as the boundaries between work and non-work time and space have become increasingly blurred, abetted by changes in technology and social norms.[15] In recent years, employers' access to or monitoring of employees' personal email or social media accounts, even if employees have accessed such accounts using firm-provided computers and

11 *Id.* at 2.

12 18 U.S.C. § 2511(2)(a)(1) (providing that it is not unlawful for "a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service . . . ."); 18 U.S.C. § 2701(c)(1) (providing that "the person or entity providing a wire or electronic communications service" may " intentionally access[ ] without authorization a facility through which an electronic communication service is provided" or "intentionally exceed[ ] an authorization to access that facility"). An employer's monitoring of communications may also be lawful because it does not fall within the Electronic Communications Privacy Act's definition of "interception." See *Fraser v. Nationwide Mutual Ins. Co.*, 352 F.3d 107 (3d Cir. 2003) (holding, in relevant part, that employer's accessing former employee's emails was not an unlawful "interception" of the emails, because the access did not occur "contemporaneously" with the emails' being sent or received).

13 See Restatement of Employment Law § 7.03. E.g. *City of Ontario v. Quon*, 560 U.S. 746 (2010) (holding that even if a police officer had a reasonable expectation of privacy with respect to personal text messages sent and received on his employer-issued pager, the public employer's review of those messages was lawful under the Fourth Amendment "[b]ecause the search was motivated by a legitimate work-related purpose, and because it was not excessive in scope"); *Hilderman v. Enea TekSci, Inc.*, 551 F. Supp. 2d 1183 (S.D. Cal 2008) (granting, in relevant part, defendant's motion for summary judgment against counterdefendant's counterclaim for invasion of privacy, because the computer accessed by defendant was defendant's property, and defendant "did not look at the computer for the purpose of rooting out personal information about [counterdefendant], but, rather, was motivated by a desire to protect its confidential information and to ensure that [counterdefendant] was not engaged in unauthorized activity that would harm [defendant].").

14 E.g. *Bingham v. Baycare Health Sys.*, Case No: 8:14-cv-73-T-23JSS, 2016 WL 3917513 (M.D. Fla. July 20, 2016) (determining that emails between plaintiff and plaintiff's attorneys produced by plaintiff's employer to defendant in response to a discovery request were not privileged, where plaintiff's employer's computer usage policy vitiated any reasonable expectation of confidentiality in the emails).

15 See Lisa M. Durham Taylor, *The Times They Are A-Changin': Shifting Norms and Employee Privacy in the Technological Era*, 15 Minn. J. L. Sci. & Tech. 949 (2014).

browsers, has been condemned, or employers' use of the information gleaned has been limited.[16] Businesses also have faced difficulties due to their "bring your own device" policies, among other employer efforts to leverage employees' own resources for business purposes.[17]

While egregious employer behavior with respect to employee personal data rightfully may be condemned, from a compliance perspective the blurring line between work and non-work spheres mean that risk monitoring and management might be justified in expanding to some degree. For example, where a company's employees use social media accounts as part of their work, it is difficult to argue that the company should not have the ability to monitor those same accounts — even if they are "personal" ones — if the business is to effectively monitor employees' competitive conduct.[18] Not only would a failure to monitor those accounts increase the risk of unlawful conduct going undetected — harming consumers — but it also would increase the risk that prosecutors would consider antitrust compliance efforts by the business insufficient, because those efforts might not be seen as appropriately tailored to the operations of the business or appropriately thorough in sampling risky activity.[19]

B. The California Consumer Privacy Act: New Protections for Privacy in the Workplace, New Problems for Effective Compliance?

Although difficult to generalize, and applied in an *ex post* fashion, the reasonable expectations rule allows for a balancing of employer and employee interests, and flexibility in achieving compliance goals — flexibility that is presumed by the DOJ's new crediting policy and guidelines. Advocates of increased privacy protection, however, have sought to increase, *ex ante*, limits on data collection and usage, and legislatures have begun to respond to their concerns. The recently-enacted California Consumer Privacy Act ("CCPA") represents this more aggressive approach to protecting individuals' personal information, and it raises important concerns for implementing the Department of Justice's guidance.

Beginning January 2020, "consumers" within the meaning of the CCPA will be able to ask a company what "personal information" the company has collected about them, and furthermore will have the right to force the company to delete the information or to prohibit the company from selling the information to third parties.[20] The CCPA has a broad jurisdictional reach, applying to companies doing business in California that either: (1) have more than $25 million in gross revenue; (2) have data on more than 50,000 "consumers," households, or devices; or (3) make over half of their revenue selling "consumer's" personal information.[21] The CCPA defines "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[22] Most critically, the law defines a "consumer" as any "natural person who is a California resident."[23]

While protecting consumer information, in general, is a worthy policy goal, the law's effective reach evidently goes beyond shielding the privacy of businesses' customers. The law's definition of a "consumer" applies to individuals beyond the ordinary meaning of the term, such as employees and job applicants – individuals who arguably should have been beyond the scope of the CCPA given the different nature of their relationships with covered business entities. Recognizing this apparent overreach, the California recently enacted Assembly Bill 25 ("AB-25").[24] AB-25 exempts information collected by a business about a natural person "acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business" from many of the CCPA's provisions, including consumers' statutory data

16 E.g. *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 759 F.Supp.2d 417 (S.D.N.Y. 2010) (holding that former employer's accessing former employee's Gmail, Hotmail, and Warrior Fitness Boot Camp email accounts using login information left on the former employer's computer violated the Stored Communications Act); *Stengart v. Loving Care Agency*, 201 N.J. 300, 990 A.2d 650 (2010) (holding that former employee "could reasonably expect that e-mail communications with her lawyer through her personal [web-based email] account would remain private, and that sending and receiving them via a company laptop did not eliminate the attorney-client privilege that protected them," and that the former employer's counsel breached the New Jersey Rules of Professional Conduct by reading the emails and failing to notify the former employee).

17 See generally Lindsey Blair, *Contextualizing Bring Your Own Device Policies*, 44 J. Corp. L. 151 (2018).

18 *Cf.* Office of Public Affairs, U.S. Dep't of Justice, President of E-Commerce Company Pleads Guilty to Price Fixing (April 11, 2019), available at https://www.justice.gov/opa/pr/president-e-commerce-company-pleads-guilty-price-fixing (announcing guilty plea of an e-commerce company president, who had engaged in a conspiracy to fix the prices of customized promotional products that was carried out through Facebook, as well as Skype and WhatsApp).

19 DOJ, Evaluation of Corporate Compliance Programs, *supra* note 6, at 7-8, 10-11.

20 See Cal. Civ. Code § 1798.100 *et seq.* (effective Jan. 1, 2020).

21 Cal. Civ. Code § 1798.140(c).

22 Cal. Civ. Code § 1798.140(o)

23 Cal. Civ. Code § 1798.140(g).

24 A.B. 25, 2019-2020 Leg., Reg. Sess., 2019 Cal. Stat. ch. 763.

deletion right.[25]

While AB-25 will improve the CCPA's approach to employers' compliance efforts, it nevertheless has important limitations. Chief among these is that AB-25's exemption for employee information will only last until January 1, 2021.[26] This means that, over the long term, companies subject to the CCPA still may have to defend whether personal information they have collected from their employees should not be subject to deletion,[27] and to defend whether the use of that information either is not limited by the law or is consistent with it.[28] These aspects of the laws pose short- to medium-term investigation and enforcement risks for businesses that they may weigh more heavily than the long-term benefits of implementing robust compliance, and thus businesses may not invest in the latter despite the DOJ's new emphasis on compliance and the protections compliance generally can offer.

In addition, even during AB-25's brief exemption period, the law does *not* relieve companies of their obligation to inform employees and job applicants "at or before the point of collection" of the kinds of personal information that will be collected and the uses to which that information may be put.[29] This seems to mean that companies must affirmatively disclose what information will be collected from employees via employer provided technology, including phones and laptops, and set forth the uses to which it may be put. This requirement effectively asks companies to predetermine what information will be relevant to compliance monitoring and auditing, without those companies knowing what personal information employees may actually put on their work devices — the kind of untailored compliance program design disfavored by the DOJ. Because of the CCPA's further requirement that companies looking to collect and use new types of personal information must re-notify "consumers" of the changes, businesses may be inclined not to modify their initial decisions, again undercutting the DOJ's policy by limiting the experience-based adjustments the DOJ has said are a hallmark of effective compliance.

C. The GDPR and Repercussions for Compliance Programs, Generally

The CCPA's forceful approach to privacy is reminiscent of the General Data Protection Regulation ("GDPR") enacted by the European Union in 2016.[30] Like the CCPA, the GDPR creates strong protections for a wide array of EU residents' personal information, including limits on such information's collection and use. Also, like the CCPA, the GDPR seems to have been designed solely with privacy in mind, creating barriers for the effective enforcement of other legal regimes through voluntary self-policing.

The GDPR's implications for compliance have been most extensively examined in the context of anticorruption efforts. TRACE International, a globally recognized anti-bribery business association, has concluded that "many GDPR provisions do not facilitate – and are even in direct conflict with – the essential elements of anti-bribery compliance programs such as due diligence of third parties and compliance procedures for monitoring, internal investigations and reporting."[31] For example, the GDPR's prohibition of the processing of personal data relating to criminal offenses inhibits data collection and analysis that is central to effective anti-bribery compliance – namely, determining whether counterparties have bribery or economic crimes convictions that make them risky transaction partners.[32] In addition, the GDPR limits the lawful bases for processing personal data, and subjects data collection to purpose and time limitations, which have not been part of anti-bribery compliance best practices.[33] These restrictions imposed by the GDPR thus present businesses with a quandary when they seek to engage in anticorruption due diligence: to the extent that they depart from compliance best practices, businesses raise their risk of exposure to corruption, but to the extent

25 A.B. 25 § 2 (amending Cal. Civ. Code. §1798.145(g)); see also A.B. 25 § 2.1 (amending Cal. Civ. Code. §1798.145(h)), § 2.2 (amending Cal. Civ. Code. §1798.145(g)), and § 2.3 (amending Cal. Civ. Code. §1798.145(h)).

26 A.B. 25 § 2.

27 Cal. Civ. Code § 1798.105(d) (stating that a business is exempt from complying with a "consumer's" request to delete information, if the information is "necessary" to achieve certain specified purposes).

28 See Cal. Civ. Code § 1798.145(a) (providing that the CCPA does not restrict a business's ability to comply with applicable law, or a civil, criminal, or regulatory, inquiry, or cooperate with law enforcement agencies concerning conduct that the business believes may violate the law).

29 A.B. 25 § 2.

30 Council Regulation 2016/679, 2016 O.J. (L. 119) 1.

31 TRACE International, Inc., Submission to OECD Working Group on Bribery 81-82, *in* OECD Working Group on Bribery, Public Comments: Review of the 2009 Anti-Bribery Recommendation (2019), available at http://www.oecd.org/corruption/anti-bribery/Public-Comments-Review-OECD-Anti-Bribery-Recommendation.pdf.

32 *Id.* at 84. See Council Regulation 2016/679 art. 10, 2016 O.J. (L. 119) 39.

33 TRACE International, Inc., Submission to OECD Working Group on Bribery 85, 87. See Council Regulation 2016/679 arts. 5-6, 2016 O.J. (L. 119) 35-37.

that they try to collect and use personal information to carry out effective due diligence, they raise their risk of a privacy enforcement action, or even a private lawsuit for a putative privacy violation.[34]

The GDPR's implications for anticorruption compliance likely are not dissimilar to their potential effect on antitrust compliance. The GDPR's provisions either prevent outright the collection and analysis of information appropriately considered as part of competition crime prevention, or discourage the collection and analysis of information that could aid detection and mitigation efforts. For companies engaged in business in both the United States and the European Union, this raises the risk of not being able to fully implement the DOJ's hallmarks of effective compliance across the board, and thus the risks of anticompetitive conduct occurring undetected and of adverse prosecutorial decisions. In addition, the GDPR presents a significant hurdle to any effort to export an American-style approach to antitrust compliance to the EU, as the GDPR provides relatively limited circumstances for modifications of its protections on a national level.[35] As a result, businesses and enforcers are disadvantaged in their efforts to protect consumers from anticompetitive actions in the market.

IV. NAVIGATING THE CROSSCURRENTS OF PRIVACY PROTECTION AND EFFECTIVE COMPLIANCE

Privacy is an important value, but to date it largely has overridden others as legislatures have considered and enacted laws to strengthen protections for personal information, thereby threatening to undercut antitrust enforcers' new efforts to incentivize and reward effective compliance programs. Governments seeking to increase privacy protections should recognize the importance of voluntary corporate self-policing when enacting or amending privacy legislation: effective antitrust compliance programs are vital to achieving government policy priorities and protecting consumers and businesses from harmful market conduct. As the implementors of both antitrust compliance programs and many privacy protections, members of the legal community and businesses have a key role to play in raising legislators' awareness of the potential privacy and antitrust law conflict, and in helping to develop solutions that harmonize the fields. Lawyers, compliance experts, and businesses can speak directly to the ways in which increased privacy protections, without tailoring, can raise the risk of anticompetitive conduct going undetected, causing harm to consumers and creating legal risks for the enterprises. They also can explain the strain on resources that can occur in trying to satisfactorily carry out competing privacy and antitrust mandates, producing suboptimal privacy and antitrust outcomes.

One way legislators could work to advance antitrust compliance, while still increasing privacy protections in general, would be to provide by law that data collection by employers from their employees for compliance purposes is a valid exception to otherwise applicable restrictions on personal information monitoring and analysis. In the United States, this could in effect maintain the reasonableness rule that has been applied to date. Legislators also could provide that government entities to which privacy regulation and enforcement are delegated must consult with other agencies, including antitrust enforcers, so that those agencies are able to ensure privacy regulators take account of their policy interests.

To the extent that these and other solutions are not implemented, however, businesses should resist the temptation to avoid instituting as many effective compliance measures as possible. New privacy regulations may make antitrust compliance more difficult, but such difficulty would not be a satisfactory justification for inaction if antitrust enforcers consider filing charges against a business. TRACE's Illya Antonenko has offered similar advice regarding anticorruption due diligence in the wake of the GDPR.[36] As Antonenko has suggested for anticorruption efforts, companies should attempt to reconcile their antitrust compliance policies and procedures with the privacy law's requirements: companies should commit time and resources to understanding their privacy law obligations, and use those requirements to frame their antitrust compliance efforts.[37] In so doing, businesses have the opportunity to protect against downside risks under both the privacy and the antitrust laws.

34 See Council Regulation 2016/679 ch. VIII, 2016 O.J. (L. 119) 80-83 (providing rights for data subjects to lodge complaints against companies with supervisory authorities, and to effective judicial remedies).

35 See Council Regulation 2016/679 art. 23, 2016 O.J. (L. 119) 46-47.

36 Ilya Antonenko, *Reconciling Personal Data Protection and Business Transparency Compliance*, CEP Magazine, Oct. 2019, at 23, 25, available at https://assets.corporatecompliance.org/Portals/1/PDF/ComplianceEthicsQuiz/CEU-articles/2019/cep-2019-10-CEU-antonenko.pdf.

37<<<< *Id.* at 23-24.

CPI COMPETITION POLICY INTERNATIONAL

CPI Subscriptions

CPI reaches more than 20,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.