Table of Contents

Overview

FOR MANDATORY SUBMISSION TO NLRB GENERAL COUNSEL, PER MEMO GC-21-04

Mandatory Submission to Advice, NLRB Memorandum GC 21-04 (Aug 12, 2021)

"Over the past several years, the Board has made numerous adjustments to the law, including a wide array of doctrinal shifts. These shifts include overruling many legal precedents which struck an appropriate balance between the rights of workers and the obligations of unions and employers. At the same time, there are many other issues that also should be carefully considered to determine whether current law ensures that employees have the right to exercise their fundamental Section 7 rights both fully and freely. Submissions of these topics to Advice will allow the Regional Advice Branch to reexamine these areas and counsel the General Counsel's office on whether change is necessary to fulfill the Act's mission.

1) Cases involving board doctrinal shifts
- Cases involving the applicability of *The Boeing Co.*, 365 NLRB No. 154 (2017), (imposing a new framework for determining the legality of workplace/employee handbook rules).
- Cases involving the applicability of *AT&T Mobility*, 370 NLRB No. 121 (2021) (overruling prong three of *Lutheran Heritage Village-Livonia*, 343 NLRB 646 (2004), and finding that an otherwise lawful work rule applied to restrict Section 7 activity remains lawful and that rescission of such rule in those circumstances is inappropriate).
- Cases involving applicability of *Rio All-Suites Hotel and Casino*, 368 NLRB No. 143 (2019) (overruling *Purple Communications*, 361 NLRB 1050 (2014) governing employees' rights to use an employer's email system for workplace communications). Regions should also submit cases involving employees' use of other electronic platforms in the workplace, i.e. Discord, Slack, Groupme, or other employer communication systems.

2) Other areas and initiatives
- Cases involving the applicability of *United States Postal Service*, 371 NLRB No. 7 (2021) (Board refusing to find a pre-disciplinary interview right to information, including the questions to be asked in the interview, as a purported extension of *Weingarten*).
- Cases involving the applicability of *Weingarten* principles in non-unionized settings as enunciated in *IBM Corp*., 341 NLRB 1288 (2004).

3) Other case-handling matters traditionally submitted to Advice
- Cases involving the need to harmonize the NLRA with local, state, or other federal statutes.
- Cases involving potential or overlapping jurisdiction with other Federal agencies, unless there is an inter-agency memorandum of understanding.

4) In addition, other yet-to-be-considered policy issues will undoubtedly arise. Regions should be sensitive to the need to submit such issues to Advice

NLRA & Surveillance

Section 8(a)(1) of the Act makes it an unfair labor practice for an employer "to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in Section 7" of the Act. For example, you may not

- Spy on employees' union activities. ("Spying" means doing something out of the ordinary to observe the activity. Seeing open union activity in workplace areas frequented by supervisors is not "spying.")
- Create the impression that you are spying on employees' union activities.
- Photograph or videotape employees engaged in peaceful union or other protected activities.
- Promulgate, maintain, or enforce work rules that reasonably tend to inhibit employees from exercising their rights under the Act.

https://www.nlrb.gov/about-nlrb/rights-we-protect/the-law/interfering-with-employee-rights-section-7-8a1

National Captioning Institute, Inc., 368 N.L.R.B. No. 105, 2019
It is well settled that an employer commits unlawful surveillance if it acts in a way that is out of the ordinary in order to observe union activity, and the board has found such intentional monitoring of pro-union employees' Facebook postings to violate federal labor law, the NLRB finds.
NCI violated §8(a)(1) by: Engaging in surveillance of employees' Union and other protected activities in emails, chat room logs and other electronic communications since May 9, 2016.

NLRB, Board Decision, The Boeing Company, 365 (2017)
The National Labor Relations Board orders that the Respondent, The Boeing Company, Renton and Everett, Washington, and Portland, Oregon, its officers, agents, successors, and assigns, shall
1. Cease and desist from (b) Creating the impression that its employees' union and/or protected concerted activities are under surveillance
The test for determining whether an employer has created an impression that its employees' protected activities have been placed under surveillance is "whether the employees would reasonably assume from the employer's statements or conduct that their protected activities had been placed under surveillance." Greater Omaha Packing Co., 360 NLRB 493, 495 (2014); Rood Industries, 278 NLRB 160, 164 (1986). When an employer tells employees that it is aware of their protected activities, but fails to tell them the source of that information, it violates Section 8(a)(1) "because employees are left to speculate as to how the employer obtained the information, causing them reasonably to conclude the information was obtained through employer monitoring."
In determining whether an employer has unlawfully created the impression of surveillance of employees' union activities, the test is whether under all the relevant circumstances, reasonable employees would assume from the statement in question that their union or other protected activities had been placed under surveillance. Frontier Telephone of Rochester, Inc., 344 NLRB 1270, 1276 (2005). The essential focus has always been on the reasonableness of the employees' assumption that the employer was monitoring their union or protected activities. Id. As with all conduct alleged to violate Section 8(a)(1) , the critical element of reasonableness is analyzed under an objective standard.

Intertape Polymer Corp. v. NLRB, 801 F. 3d 224 2015

The exception to this general rule arises when the employer's observation of union activities can be reasonably construed as excessive or coercive surveillance, such that it "unreasonably chill[s] the exercise of the[] employees' Section 7 rights." *NLRB v. Southern Md. Hosp. Ctr.,* 916 F.2d 932, 938 (4th Cir.1990) (per curiam) (noting that "the Board has on several occasions found that employers unreasonably chilled the exercise of their employees' Section 7 rights through *excessive* surveillance") (emphasis added); *cf. Arrow-Hart, Inc.,* 203 N.L.R.B. 403, 403 (1973) (noting that an employer's act of "coercively surveilling — that is, spying upon — its employees' activities" would be a violation of the Act). As stated previously, the employer's observation must have a "reasonable tendency in the totality of the circumstances to intimidate" the employees. *Nueva Eng'g.,* 761 F.2d at 965.
This is because, "[w]hen an employer watches ... employees because he believes they are engaged in union activities, the employees may reasonably fear that participation in union activities will result in their identification by the employer as union supporters." *Id.* at 967. The "employee, possibly anticipating retaliation against identified supporters, may thereafter feel reluctant to participate in union activities." *Id.*; *see also NLRB v. Grand Canyon Mining Co.,* 116 F.3d 1039, 1045 (4th Cir.1997) ("[A]n employer violates section 8(a)(1) of the Act if it gives employees the impression that it is conducting surveillance of their union activities."); *J.P. Stevens & Co.,* 638 F.2d at 683 ("It is an unfair labor practice for an employer to create in the minds of employees an impression that he is closely observing union organizational activity."). Such excessive or coercive "surveillance becomes illegal because it indicates an employer's opposition to unionization, and the furtive nature of the snooping tends to demonstrate spectacularly the state of the employer's anxiety." *Belcher Towing,* 726 F.2d at 708 n. 2. "From this the law reasons that when the employer either engages in surveillance or takes steps leading his employees to think it is going on, they are under the threat of economic coercion." *Id.*
Ultimately, "[t]he test for determining whether an employer engages in unlawful surveillance, or unlawfully creates the impression of surveillance, is an objective one and involves the determination of whether the employer's conduct, under the [totality of the] circumstances, was such as would tend to interfere with, restrain, or coerce employees in the exercise of their rights guaranteed under Section 7 of the Act." *Southern Md.,* 916 F.2d at 938 (internal quotation marks omitted); *cf. Nueva Eng'g.,* 761 F.2d at 965 (The employer's conduct must have a "reasonable tendency in the totality of the circumstances to intimidate" the employees.).
For example, we consider "the duration of the observation, the employer's distance from its employees while observing them, and whether the employer engaged in other coercive behavior during its observation." *Aladdin Gaming, LLC,* 345 N.L.R.B. 585, 586 (2005). But we must also consider whether the employer had a legitimate reason for observing the activities or for otherwise being present at the place where the alleged surveillance has occurred. *See, e.g., Nueva Eng'g.,* 761 F.2d at 967 (upholding violation where two supervisors went to an off-site location "for the purpose of surveilling a scheduled union meeting" and, "when no meeting occurred, the supervisors followed three employees to an employee's home"); *Sprain Brook Manor Nursing Home, LLC,* 351 N.L.R.B. 1190, 1191 (2007) (finding unlawful surveillance where nursing home administrator went to facility on her day off "solely for the purpose of observing union activity" and stood in the doorway closest to where the union organizer was meeting with the employees so as to be able to see the employees and be seen by them); *PartyLite Worldwide, Inc.,* 344 N.L.R.B. 1342, 1342 (2005) (finding unlawful surveillance of union handbilling activities because, "on three separate occasions shortly before the election, no less than eight high-ranking managers and supervisors stood at entrances to the employee parking lot watching the [union] give literature to employees as they entered and exited the parking lot during shift changes," "the presence of managers and supervisors at the entrances to the parking lot was surprising

and an unusual occurrence," and "[t]he employer established no legitimate explanation for why any of its managers and supervisors were stationed in the parking lot during the [Union's] handbilling activities"); *S.J.P.R., Inc.,* 306 N.L.R.B. 172, 172 (1992) (finding that the employer "engaged in unlawful surveillance by posting one or two security guards near the employee entrance and another security guard with binoculars in an upstairs hotel room in order to observe employees and union agents soliciting union authorization card signatures across the street from the hotel," because it "constituted more than ordinary or casual observation of public union activity" and "[t]here [was] no evidence that the [employer's] conduct was based on safety or property concerns"); *Eddyleon Chocolate Co.,* 301 N.L.R.B. 887, 888 (1991) (finding violation where supervisor "drove his car to within 15 feet of" the union representative, "watched employees as [the union representative] handed them literature ... near the entrance to the [employer's] parking lot," and "spoke into his car telephone" until the union representative left); *Arrow Auto. Indus.,* 258 N.L.R.B. 860, 860-61 (1981) (finding unlawful surveillance of union handbilling activities where "[s]oon after the handbilling began on 2 of the 3 days ... in question, 11 of the [employer's] supervisors lined up in varying numbers near each of the three gates, observing the employees as they drove past the union handbillers," "the presence of the supervisors was highly unusual," "the supervisors' presence was deliberately calculated to show and demonstrate observation in numbers and force," and the employer failed to demonstrate a legitimate reason for being there) (internal quotation marks, alterations, and footnotes omitted).

Purple Communications, 361 NLRB No. 126 , (2014)

We acknowledge that employers who choose to impose a working-time limitation will have concerns about the extent to which they may monitor employees' email use to enforce that limitation. Our decision does not prevent employers from continuing, as many already do, to monitor their computers and email systems for legitimate management reasons, such as ensuring productivity and preventing email use for purposes of harassment or other activities that could give rise to employer liability.**73** The Respondent and some amici assert that such monitoring may make them vulnerable to allegations of unlawful surveillance of employees' Section 7 activity. We are confident, however, that we can assess any surveillance allegations by the same standards that we apply to alleged **[*1065]** surveillance in the bricks-and-mortar world. Board law establishes that "those who choose openly to engage in union activities at or near the employer's premises cannot be heard to complain when management observes them. The Board has long held that management officials may observe public union activity without violating the Act so long as those officials do not 'do something out of the ordinary.'" An employer's monitoring of electronic communications on its email system will similarly be lawful so long as the employer does nothing out of the ordinary, such as increasing its monitoring during an organizational campaign or focusing its monitoring efforts on protected conduct or union activists. Nor is an employer ordinarily prevented from notifying its employees, as many employers also do already, that it monitors (or reserves the right to monitor) computer and email use for legitimate management reasons and that employees may have no expectation of privacy in their use of the employer's email system.

F. W. Woolworth Co., 310 NLRB 1197 (1993)

A]n employer's mere observation of open, public union activity on or near its property does not constitute unlawful surveillance. Photographing and videotaping such activity clearly constitute more than mere observation, however, because such pictorial record keeping [*65] tends to create fear among employees of future reprisals. The Board in Woolworth reaffirmed the principle that photographing in the mere belief that something might happen does not justify the employer's conduct to interfere with

employees' right to engage in concerted activity . . . . Rather, the Board requires an employer engaging in such photographing or videotaping to demonstrate that it had a reasonable basis to have anticipated misconduct by the employees. "[T]he Board may properly require a company to provide a solid justification for its resort to anticipatory photographing . . . . The inquiry is whether the photographing or videotaping has a reasonable tendency to interfere with protected activity under the circumstances in each case.

NLRB v. Southern Md. Hosp. Ctr., 916 F.2d 932, 938 (4th Cir.1990)
The test for determining whether an employer engages in unlawful surveillance, or unlawfully creates the impression of surveillance, is "an objective one and involves the determination of whether the employer's conduct, under the circumstances, was such as would tend to interfere with, restrain, or coerce employees in the exercise of their rights guaranteed under Section 7 of the Act."
Applying that test, the Board has on several occasions found that employers unreasonably chilled the exercise of their employees' Section 7 rights through excessive surveillance. See Arthur Briggs, Inc., 265 NLRB 299, 309 (1982) (unlawful surveillance because employer's representative went outside employer's property to observe union activity), enf'd mem., 729 F.2d 1441 (2d Cir.1983); Arrow Automotive Industries, 258 NLRB 860, 861 (1981) (employer's surveillance of public handbilling was "deliberately calculated plan to show and demonstrate observation, in numbers and force, and its cause and effect was the surveillance of the employees"), enf'd mem., 679 F.2d 875 (4th Cir.1982); Montgomery Ward & Co., 256 NLRB 800, 812 (1981) (employer interfered with organizers during meeting and engaged in "unreasonably close" observation of organizers as they finished their lunches), enf'd, 692 F.2d 1115 (7th Cir.1982), cert. denied, 461 U.S. 914, 103 S.Ct. 1892, 77 L.Ed.2d 282 (1983). In all these cases, however, the union representatives possessed the Section 7 right to engage in the particular organizational activities. In Arthur Briggs, Inc., for example, the union representatives were legally entitled to distribute handbills outside the employer's property, see 265 NLRB at 309; in Arrow Automotive Industries, the organizers had the right to handbill prospective members in the plant parking lot, see 258 NLRB at 863; and in Montgomery Ward & Co., the nonemployee union organizers were lawfully, unlike the instant case, in the company's cafeteria when they solicited employees, see 256 NLRB at 812.

NLRB v. Grower-Shipper Vegetable Assn. of Central California (1941)
Prohibits “out-of-the-ordinary” surveillance of union activity regardless if the workers are aware of it. That precedent lacks “meaningful analysis” about how an employer can interfere with, restrain, or coerce employees’ exercise of their rights under federal labor law if they don’t know about the surveillance.

Apple Searches & Privacy Policy Violating NLRA § 7 Rights

Policy: Workplace Searches and Privacy [1]
https://people.apple.com/US/en/subtopic/845

"In order to protect Apple confidential and sensitive[2] information and maintain the security and integrity of our networks and equipment, any use of Apple property, as well as use of your personal devices for Apple business or for accessing Apple networks, is subject to this policy."

"Workplace searches [3]
Only in cases where allowed under local law, [4] Apple may:

- Access, search, monitor, archive, and delete Apple data stored on all of its property, as well as non-Apple property, if used for Apple business or if used for accessing Apple data, servers, or networks. This includes all data and messages sent, accessed, viewed, or stored (including those from iCloud, Messages, or other personal accounts) using Apple equipment, networks, or systems.
- Conduct physical, video, or electronic surveillance, search your workspace such as file cabinets, desks, and offices (even if locked), review phone records, or search any non-Apple property (such as backpacks, purses) on company premises."

"This means that you have no expectation of privacy when using your or someone else's personal devices for Apple business, when using Apple systems or networks, or when on Apple premises."

"The search or removal of Apple-related content on a device will be determined on a case-by-case basis when there is a business need and subject to local approval processes. Refusing to permit a search or removal of Apple-related content may result in disciplinary action up to and including termination of employment." [5]

[1] Photographing employees engaged in protected concerted activities constitutes unlawful surveillance because it has a tendency to intimidate employees and interfere with exercise of Section 7 rights. Photographing in the mere belief that something "might" happen is not a sufficient justification. *F.W. Woolworth Co.*, 310 NLRB 1197 (1993); see also, *National Steel and Shipbuilding Co.*, 324 NLRB 499 (1997) (peaceful union rallies); *Labor Ready, Inc.*, 327 NLRB 1055 (1999), (employer videotapes of workers employed by temporary service in waiting room waiting for assignments unlawful).
[2] Note: Overbroad
[3] *Boeing Corporation Advice Memo (2013),* Boeing must cease and desist from creating the impression that its employees' union and/or protected concerted activities are under surveillance. *Register Guard,* 344 NLRB 1142, 1144 (2005) (test is whether the employee would reasonably assume from the statement that their union activities had been placed under surveillance*." Flexsteel Industries*, 311 NLRB 257, 257 (1993).
[4] Note: Overbroad
[5] Note: Overbroad. Do organizing and union materials count as Apple-related?

Memo from Apple CEO

Date: Sept 21, 2021
From: Tim Cook, To: Apple_Employees$@group.apple.com
Subject: Follow-up on global team meeting

Excerpt:

I want you to know that I share your frustration. These opportunities to connect as a team are really important. But they only work if we can trust that the content will stay within Apple. I want to reassure you that we are doing everything in our power to identify those who leaked.[6] As you know, we do not tolerate disclosures of confidential information, whether it's product IP or the details of a confidential meeting.[7] We know that the leakers constitute a small number of people. We also know that people who leak confidential information do not belong here.[8] [9] [10] [11]

[6] *Register Guard,* 344 NLRB 1142, 1144 (2005) (test is whether the employee would reasonably assume from the statement that their union activities had been placed under surveillance." *Flexsteel Industries, 311 NLRB 257, 257 (1993),*

[7] "[I]f something is not public information, you must not share it." We determined that the following confidentiality rules were facially unlawful, even though they did not explicitly reference terms and conditions of employment or employee information, because the rules contained broad restrictions and did not clarify, in express language or contextually, that they did not restrict Section 7 communications: *Report of the General Counsel Concerning Employer Rules, NLRB Memorandum GC 15-04 (2015)*

[8] *Yale New Haven Hospital*, 309 NLRB 363, 368 (1992) (supervisor unlawfully threatened employee with reprisal by telling an employee that if he did not stop protected activities he would "talk" to him again; implies that the talk will not be mere conversation but will concern the employment of the offending employee).

[9] *Valerie Manor,Inc.,*351NLRB1306(2007)(threat of unspecified reprisals).

[10] *Equipment Trucking Co.,Inc*.,336NLRB277(2001)(statement, If you don't like it, find another job, implied threat of discharge).

[11] *Medco Health Solutions Of Las Vegas, Inc.*,357NLRBNo.25(2011) (respondent's statement that, if employee could not support the respondent's policies, there were other jobs out there and perhaps "this wasn't the place for him" was an implied threat in violation of 8(a)(1)).

Apple Surveillance Patents

I. Patent: Systems and methods for identifying unauthorized users of an electronic device

Patent: US20100207721 A1
Application: 2009; Granted: 2012; Expires: 2031

EFF slams Apple patent as traitorware: Jobs is spying on you?
By Darlene Storm, Computerworld | AUG 24, 2010 3:09 PM PST
https://www.computerworld.com/article/2469001/eff-slams-apple-patent-as-traitorware--jobs-is-spying-on-you-.html

> When you personally buy a new technological toy, then it's yours to do with as you please. Right? Wrong! What if your new device were activated on the sly and used against you? That's a step beyond spyware. In fact, the EFF coined a new term, "traitorware."
> Unless you've been cut off from technology, then you have probably heard about Apple's patent, "Systems and Methods for Identifying Unauthorized Users of an Electronic Device." It appears that Apple is taking steps to enable locking out unauthorized iOS users. What's new is that privacy watchdog EFF has posted their reaction to this Apple patent application. I love the EFF, so I listen when they talk.
> The EFF weighed in on Apple's recent security software patent. The EFF's post, Steve Jobs Is Watching You: Apple Seeking to Patent Spyware, states, "This patent is downright creepy and invasive - certainly far more than would be needed to respond to the possible loss of a phone. Spyware, and its new cousin traitorware, will hurt customers and companies alike - Apple should shelve this idea before it backfires on both it and its customers."
> From a security perspective, Apple has Mobile Me that allows users to find a lost iPhone or iPad via a web portal. The app will approximately map where the device is currently located. It allows a user to play a sound even if it's off. It allows users who do not want the information on their Apple device to fall into enemy's hands, or into anyone's elses, to remotely erase the device. So why does Apple need an enhanced version of Mobile Me?
> According to Patent Vest, this Apple patent is aimed at identifying unauthorized users. Your iPhone might identify you through its camera or through its microphone, to verify if you are indeed the owner. It might user a biometric measurement, such as detecting the heartbeat to make sure it matches the authorized user's "heart signature." It could log keystrokes and GPS coordinates, and could even measure "vibration profiles," whatever that really means.
> Depending upon how you view those security matters, you might cheer Apple's ingenuity. Or you may, like the EFF, feel like Steve Jobs is spying on you with traitorware. Apple would surely make this software opt-in. But then again, what jailbreaking fan in their right mind would opt-in when this software would also be able to detect your jailbroken or hacked Apple devices? If you wanted to jailbreak your iPhone or iPad, then why wouldn't you stick with Mobile Me if you lost your Apple toy? Will the orignial Mobile Me be discontinued?

What if you are not into jailbreaking and you are all for strong security? Do you feel confident that Apple would never be hacked and that their analysis of your face, your voice, and your heartbeat data will never become vulnerable? Calling anything unhackable is like issuing a challenge to some hackers. Perhaps in the future, a heartbeat signature will become a valuable part of your identity?
If you bought an Apple product and you want to jailbreak it, then you should be able to do so. If Apple begins to remotely wipe jailbroken devices, then it seems that is as good as announcing it doesn't want your jailbreaking business.
The most troubling part of this patent, to me, is the potential for Apple to take action against users who jailbreak. That does seem too invasive into your privacy. Using your own personal device against you may even make Apple's patent spyware a type of traitorware. Will it herald a pending iPocolypse?
I "know" Big Brother is watching, but I'm not so sure Steve Jobs is.

Steve Jobs Is Watching You: Apple Seeking to Patent Spyware
EFF JULIE SAMUELS AUGUST 23, 2010
https://www.eff.org/deeplinks/2010/08/steve-jobs-watching-you-apple-seeking-patent-0

It looks like Apple, Inc., is exploring a new business opportunity: spyware and what we're calling "traitorware." While users were celebrating the new jailbreaking and unlocking exemptions, Apple was quietly preparing to apply for a patent on technology that, among other things, would allow Apple to identify and punish users who take advantage of those exemptions or otherwise tinker with their devices. This patent application does nothing short of providing a roadmap for how Apple can — and presumably will — spy on its customers and control the way its customers use Apple products. As Sony-BMG learned, spying on your customers is bad for business. And the kind of spying enabled here is especially creepy — it's not just spyware, it's "traitorware," since it is designed to allow Apple to retaliate against you if you do something Apple doesn't like.
Essentially, Apple's patent provides for a device to investigate a user's identity, ostensibly to determine if and when that user is "unauthorized," or, in other words, stolen. More specifically, the technology would allow Apple to record the voice of the device's user, take a photo of the device's user's current location or *even detect and record the heartbeat of the device's user*. Once an unauthorized user is identified, Apple could wipe the device and remotely store the user's "sensitive data." Apple's patent application suggests it may use the technology not just to limit "unauthorized" uses of its phones but also shut down the phone if and when it has been stolen.
However, Apple's new technology would do much more. This patented device enables Apple to secretly collect, store and potentially use sensitive biometric information about you. This is dangerous in two ways: First, it is far more than what is needed just to protect you against a lost or stolen phone. It's extremely privacy-invasive and it puts you at great risk if Apple's data on you are compromised. But it's not only the biometric data that are a concern. Second, Apple's technology includes various types of usage monitoring — also very privacy-invasive. This patented process could be used to retaliate against you if you jailbreak or tinker with your device in ways that Apple views as "unauthorized" even if it is perfectly legal under copyright law.
Here's a sample of the kinds of information Apple plans to collect:

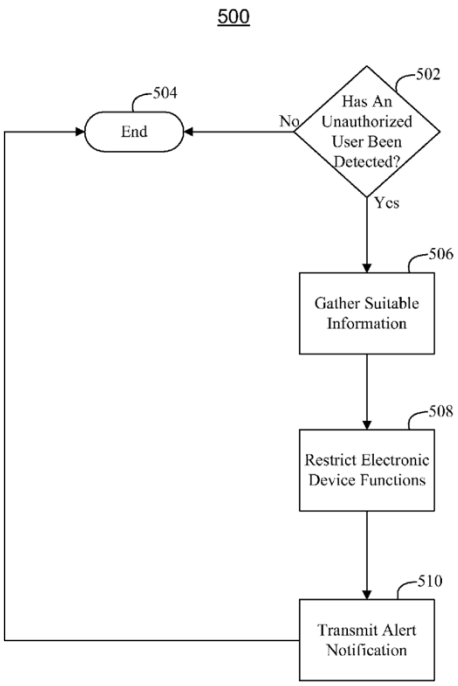
- The system can take a picture of the user's face, "without a flash, any noise, or any indication that a picture is being taken to prevent the current user from knowing he is being photographed";
- The system can record the user's voice, whether or not a phone call is even being made;
- The system can determine the user's unique individual heartbeat "signature";
- To determine if the device has been hacked, the device can watch for "a sudden increase in memory usage of the electronic device";
- The user's "Internet activity can be monitored or any communication packets that are served to the electronic device can be recorded"; and
- The device can take a photograph of the surrounding location to determine where it is being used.

In other words, Apple will know who you are, where you are, and what you are doing and saying and even how fast your heart is beating. In some embodiments of Apple's "invention," this information "can be gathered every time the electronic device is turned on, unlocked, or used." When an "unauthorized use" is detected, Apple can contact a "responsible party." A "responsible party" may be the device's owner, it may also be "proper authorities or the police."

Apple does not explain what it will do with all of this collected information on its users, how long it will maintain this information, how it will use this information, or if it will share this information with other third parties. We know based on long experience that if Apple collects this information, law enforcement will come for it, and may even order Apple to turn it on for reasons other than simply returning a lost phone to its owner.

This patent is downright creepy and invasive — certainly far more than would be needed to respond to the possible loss of a phone. Spyware, and its new cousin traitorware, will hurt customers and companies alike — Apple should shelve this idea before it backfires on both it and its customers.

New Apple tech can detect, alert iPhone owners of unauthorized use
Mikey Campbell | Oct 16, 2012
https://appleinsider.com/articles/12/10/16/new-apple-tech-can-detect-alert-iphone-owners-of-unauthorized-use



The patent's innocuous language starts out by saying, "This is generally directed to identifying unauthorized users of an electronic device," but goes far beyond any identification technology currently available in Apple's handset. For example, one embodiment of the invention calls for heartbeat monitoring, which can be used to determine whether the person holding an iPhone is its owner.

The patent essentially covers three main operations: the detection of an unauthorized user; the gathering of information of an unauthorized user; and the transmission of an alert notification to the electronic device's owner containing said information.

As mentioned above, a person's heartbeat can be used to determined whether he or she is the owner of a device, though more conventional methods are also described, such as taking a photograph or matching voice recordings.

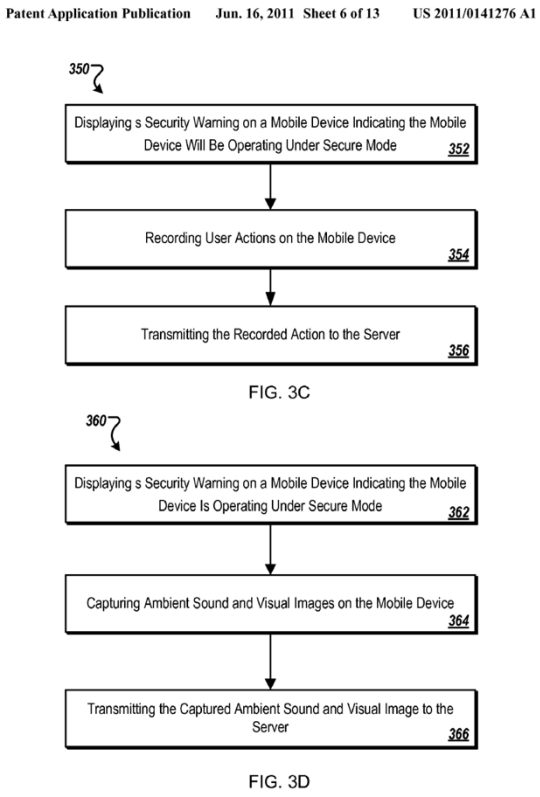
Perhaps most effective are the patent's other embodiments in which an unauthorized user is identified through a number of actions. For example, "entering an incorrect password a predetermined number of times in a row, hacking of the electronic device, jailbreaking of the

electronic device, unlocking of the electronic device, removing a SIM card from the electronic device, or moving a predetermined distance away from a synced device" can all be used as means of detection.

When a non-owner is identified, the device can enter an information gathering mode in which location, photographs, voice recordings, screenshots, keylogs, and internet usage are stored. Another option is to restrict the phone's functions and erase sensitive information when an unauthorized user takes control of the device.

Finally, an alert is sent to a "responsible party," such as the device owner or police, containing a predetermined message like "Warning, your electronic device may have been stolen." In addition, the alert, sent via text, email, instant message, or over the internet, can contain the information the device gathered when in the hands of the unauthorized user.

In some embodiments, near field communications, or NFC, can be employed to pair the handset with a key fob or similar device. If the phone moves far enough away from the key fob, it will issue a warning which will turn into a formal alert if the device moves a substantial distance.



II. Patent: Proactive Security for Mobile Devices

Patent: US 2011/0141276 A1
Application: 2009; Granted: 2016; Expires: 2032

Apple exploring 'proactive' iPhone security methods for stolen hardware
Neil Hughes | Jun 16, 2011
https://appleinsider.com/articles/11/06/16/apple_exploring_proactive_iphone_security_methods_for_stolen_hardware

Apple's new potential security options are detailed in a patent application made public this week and discovered by AppleInsider. Entitled "Proactive Security for Mobile Devices," the feature would offer extremely flexible, custom options for security measures on an iPhone.

But a user may also decide to continue to allow some features on a missing device, such as Wi-Fi or GPS, to help track down the handset and identify its location. Keeping that functionality active allows the rightful owner of the device to determine its place on a map.

Apple's solution could also utilize the sensors inside of an iPhone to record unusual activity, and alert users that their handset is at security risk, potentially preventing it from being lost forever. Such a system could detect suspicious activities like calls or texts to an unknown number.

If an iPhone is reported stolen, the device could record images and ambient audio. This data could be provided to investigative authorities to help track down the hardware.

Patent indicates sophisticated remote surveillance for Find My iPhone
9to5 Staff Jun. 16th 2011 8:24 am PT
https://9to5mac.com/2011/06/16/patent-indicates-sophisticated-remote-surveillance-for-find-my-iphone/

> So, what are the aggressive countermeasures Apple's been exploring? For starters, they propose selective protection of your content stored on the device. This would kick in when someone enters an incorrect passcode. We are more excited, however, about cool remote surveillance capabilities, such as transmission of the images and sounds that your device secretly captures. This could go a long way towards helping one figure out the thief's surrounding without them suspecting anything. Yeah, kinda like this guy. Warning: This article will self-destruct in T-minus thirty seconds…
> Apple explains: *"A mobile device can proactively determine whether the mobile device is associated with a security risk and the level of the security risk. Upon determining a security risk, the mobile device can transmit coordinates of its current geographic location to a server. To protect privacy of authorized users, the transmission can be disabled by entering a password. If multiple failed password attempts are detected, the mobile device can proactively increase a security level of the device, and selectively protect files or other content stored on the mobile device. In some implementations, the mobile device can be transitioned into a surveillance mode where the mobile device records or captures information associated with one or more of user actions, ambient sound, images, a trajectory of the device, and transmits the recorded or captured information to the network resource."* You can browse this patent application by typing in the ID number 20110141276 into the United States Patent & Trademark office search engine.

Orwellian Watch: Apple's Creepy Patent Application
RENEE ORICCHIO AUG 23, 2010
https://www.inc.com/tech-blog/orwellian-watch-apples-creepy-patent-application.html

> Apple has applied for a patent on new technology that would enable it to take control remotely and disable mobile devices (think iPhone and iPad) or wipe out data altogether. It's apparantly for the purpose of cracking down on jailbreakers and in the event the device is stolen or lost.
> On it's face, it doesn't sound terrible I suppose. If my phone were stolen, I would certainly be more concerned about the lost and compromised personal information on board falling into the wrong hands than losing the phone itself. What a relief it would be to have Apple simply erase the little sucker wherever it is and save my privacy.
> But, is this really a privacy saver or a privacy buster?
> The answer depends on how much you trust Apple, I guess. Or how intimate your relationship is with a faceless mega-corporation.
> Are you comfortable enough with Apple that it's okay for them to:
> - have the power to turn on your iPhone camera, snap a picture of whatever is in plain site of the lense and then upload it to Apple for analysis?
> - have the power to record your voice on your next phone call and upload it for analysis, as well?
> - have the power to record your heartbeat as you use your phone and... you know the rest?
>
> These are the capabilities described in the patent application entitled "Systems and Methods for Identifying Unauthorized Users of an Electronic Device". Apple would archive a picture, voice

and heartbeat recording of the authorized user up front. This would be the baseline for the above analysis scenarios.

Nevermind the obvious:

- that Apple is developing technology to crack down on jailbreaking iPhones after the courts just ruled its legal to jailbreak your own phone.

I can't resist playing the "what if" game.

So, what if...

... it's all a big misunderstanding and the camera takes a picture for the Apple mothership while you are in the middle of sexy time?

... it's all a big misunderstanding when your daughter's voice doesn't match your archived voice at the Apple nerve center? So, she's borrowed your phone. It doesn't work and now she can't call you to let you know she has a flat tire out on the Interstate.

... Oops, your archived heartbeat isn't a match and your phone is disabled right in the middle of your 911 call when you are, oh say, HAVING A HEART ATTACK? Hello!

Think I'm off base? This will never happen! What are the chances - one in a million? Perhaps! But, consider this; there are some 45 million iPhone users out there. One in a million translates to about 45 people in that one flukey situation that compromises their privacy - or worse.

Apple Surveillance Press Coverage

Worker surveillance is making employees miserable
Sarah Roach Protocol Sept 2021
https://www.protocol.com/workplace/worker-surveillance-is-making-employees-miserable

Last weekend, Ashley Gjøvik walked around her apartment unplugging all of her electronics. Apple had just fired her for allegedly leaking information, and for months before then, she had spoken out with claims of harassment, intimidation and surveillance at the company. She'd been thinking through Apple's employee privacy policy, which states that workers have no expectation of privacy when using a personal device for Apple business, and wondered if that meant the company could watch her through her home devices, too.

"I think the worst moment was realizing that they were probably watching me through my Eve cameras and listening to me on my HomePod," she told Protocol. "It was this frantic moment. I don't even have words for it yet, of how violating and horrifying and terrifying it was."

Gjøvik said Apple employees don't usually question the fact that their devices are being monitored, because workers have always figured the information collected would be used in good faith. But it wasn't until she began speaking out about the company that she started to realize it could be used against her.

Employees like Gjøvik have been raising concerns around Apple's surveillance capabilities in recent weeks, but security and privacy experts have been warning of the underlying dangers of using this technology for a long time. Experts say companies can now see the real-life toll surveillance technology takes on employees, and its ability to erode trust between managers and their workers.

"You don't even need the technology. What you need to be doing is focusing on what the employee is turning in, what the employee is saying in meetings, what the employee is telling you. I think that is far more important than metrics that most technologies are providing," said Elizabeth Lyons, who studies technology and management at the University of California San Diego.

The thing about worker surveillance technology is that even if it's meant to be used for work only, there's always a lingering feeling that managers can find out a lot of personal details, too. That was the case for Gjøvik, who has tweeted about Apple obtaining personal photos of her. "I feel silly about the fact that I put all this stuff out there and thought, 'It'll be fine.' And now I'm like, 'Oh my god, what did I do?'"

Worker surveillance tools can track keystrokes, mouse movements, which programs are open at a given time, how long someone remains on a website or apps, what someone's talking about online and more.

And Apple certainly isn't the only one possibly surveilling employees. Vice reported last month that Amazon would track the keyboard and mouse movements of its customer service employees in an effort to find people stealing private customer data. Meanwhile, managers can see live videos of Amazon drivers while they're out on the job, and the company tracks the amount of time a warehouse worker takes off during a shift.

An Amazon spokesperson declined to comment on its surveillance technology, adding that maintaining security and privacy of customer and employee data is "among our highest priorities."

Former Amazon worker Ryan Fan said he didn't mind being monitored at work; as long as he was being productive, he knew he wouldn't get in trouble. "If I was on my phone or something, I just wouldn't be on it for a long period of time just in case I was [called out]. But if I got done what I needed to do, I could, as long as I was productive. I wasn't really bothered," he told Protocol.

But other Amazon workers feel otherwise, especially those who were trying to unionize. Last year, the company reportedly bought software to help it track data on unions, and its corporate employees began monitoring hotspots for employee activism. Earlier this month, trade unions in Ireland raised concerns over worker surveillance after Amazon announced plans to open warehouses in the country.

Worker surveillance technology isn't going away anytime soon; the market for these tools is expected to boom in the next few years, potentially reaching $4.5 billion by 2026. Much of that growth is tied to the COVID-19 pandemic, as companies try to keep watch over employees while remote work continues.

Businesses that provide this technology have a few reasons for doing so. Take Time Doctor as an example: While indicating interest in its monitoring tools, the employer can choose a reason for watching over their workers, including "I don't trust my employees," "I want tools to manage my remote team," "I need to see where my employees spend their time" and "I want to keep my employees accountable."

Alan Brown, a sales manager at Controlio — which provides surveillance tools like time tracking and a livestream of employees' screens — said companies might also monitor employees to increase productivity, prevent intellectual property theft, help managers better understand what employees are working on and determine what kinds of applications are used most often.

Whatever the reason is, experts said companies should still be careful with the tools. Reid Blackman, CEO of ethics consulting firm Virtue, said companies should prepare to answer a load of questions from their employees before they implement surveillance.

"What else is it going to be used for? Who is using those monitoring tools? Who has access to the data that those monitoring tools gather? What's done with it? What's the level of transparency with workers around its use? Does it play any role in evaluations of people's work with regard to firing and promotions and bonuses?"

But even if a company is communicating with workers about the technology, surveillance still changes the power dynamic in the workplace, according to Kathryn Zickuhr, a labor market policy analyst at the Washington Center for Equitable Growth. Even if it's unintentional, monitoring a worker's every move can allow employers to learn about sensitive or personal information like health data, which can in turn create a deeper power imbalance at a company.

"Even if you have transparency and all of this, ultimately they don't have the power to opt out of this," Zickuhr told Protocol. "This really just exacerbates the power imbalances between very large employers and low-wage workers."

> Gjøvik, the former Apple employee, said companies need to take the lessons learned at Apple if and when they decide to use their own monitoring tools. She said workers should be able to demand protections over their data and transparency in how their data is being used.
> "What are you even up to, and what control do I have over my information? There could be a committee to say, 'Why do you need to access some of this stuff?'" she said.

Apple's Double Agent: He spent years inside the iPhone leaks and jailbreak community. He was also spying for Apple.
VICE | Lorenzo Franceschi-Bicchierai | August 18, 2021
www.vice.com/en/article/3aqyz8/apples-double-agent

> Shumeyko said he established a relationship with Apple's anti-leak team—officially called Global Security—after he alerted them of a potential phishing campaign against some Apple Store employees in 2017. Then, in mid-2020, he tried to help Apple investigate one of its worst leaks in recent memory, and became a "mole," as he put it.
> The secretive Global Security reportedly employs former U.S. intelligence and FBI agents and is tasked with cracking down on leaks and leakers, but very little is known about the way it operates.
> Apple has been trying to crack down on them recently by sending them legal letters, which revealed that the company knows their names and home addresses, despite the fact that they only use nicknames online.
> None of the people Shumeyko mentioned to Apple, and whom Motherboard spoke to, had any idea that Shumeyko had become a mole for the company.
> "Going forward if you plan to publish anything, please consult us (if you want to do the right things for yourself)," Apple Global Security's employee told Shumeyko.

Apple accused of monitoring employee text messages in lawsuit against ex-chip exec
CNBC | DEC 10 2019
https://www.cnbc.com/2019/12/10/apple-accused-of-monitoring-employee-text-messages-in-lawsuit-against-ex-chip-exec.html

> A former Apple executive alleges the company illegally gathered private text messages from his iPhone before firing him for breach of contract.
> Williams argues Apple illegally collected text messages between him and other Apple employees, two of which went on to be Nuvia's co-founders, to build its case.
> "Apple, an early beneficiary of the creative forces that formed and continue to drive Silicon Valley, has filed this lawsuit in a desperate effort to shut down lawful employment by a former employee," the lawsuit states. "To further intimidate any current Apple employee who might dare consider leaving Apple, Apple's complaint shows that it is monitoring and examining its employees' phone records and text messages, in a stunning and disquieting invasion of privacy."

Ex-Apple Executive Accused of Betrayal Says He Was Snooped On
Bloomberg Mark Gurman and Edvard Pettersson December 9, 2019, 5:29 PM PST
https://www.bloomberg.com/news/articles/2019-12-10/ex-apple-executive-accused-of-betrayal-says-he-was-snooped-on

> A former Apple Inc. executive who worked on the chips that power iPhones claims the company reviewed his confidential text messages before suing him for launching his own startup.
> In response, Williams accused Apple of a "stunning and disquieting invasion of privacy" over its monitoring of his texts. In one message, Williams said Apple would have "no choice but to purchase" his new company.
> In "Apple's theory, if one Apple employee speaks to (or texts) another employee conveying criticisms of Apple's strategies or decisions, that discussion is itself a purportedly unlawful 'solicitation' to leave Apple," he said in a filing.

Apple claims it isn't scanning customers' faces, after teen sues for $1 billion
Shannon Liao | Apr 23, 2019
https://www.theverge.com/tech/2019/4/23/18512942/apple-lawsuit-facial-recognition-nypd-1-billion-theft

> Apple is being accused of using facial recognition software in its Apple Stores to arrest the wrong person for theft — a New York student who's now suing Apple for $1 billion. And while Apple tells The Verge it doesn't use facial recognition technology in its stores, the case is weird enough, and there's enough wiggle room, that it's not clear if that's the whole truth.
> When we reached Reinhold on the phone for comment, he agreed that Apple doesn't technically have facial recognition in its stores, but also that his statements as described in the lawsuit were correct. He declined to answer further questions, but it's worth noting that the second defendant on the lawsuit, Security Industry Specialists, might explain the contradiction — it could have been that company which used facial recognition to analyze security footage after the fact, and possibly outside of Apple's facilities.
> SIS Security doesn't explicitly mention Apple as a client on its public website, but the third-party firm seems to have a long working relationship with Apple, and a 2016 employee handbook hosted at its website specifies Apple as a client.

What It's Like to Work Inside Apple's 'Black Site': Contractors a few miles from the company's spaceship-like headquarters live in fear of termination—and the bathroom lines.
Bloomberg | Joshua Brustein | February 11, 2019
https://www.bloomberg.com/news/features/2019-02-11/apple-black-site-gives-contractors-few-perks-little-security

> "There was a culture of fear among the contractors which I got infected by and probably spread."
> Apex, not Apple, manages the workers it hires. Apple says it requires contracting firms to treat workers with "dignity and respect." Following an inquiry from Bloomberg News, the company says, it conducted a surprise audit of the Hammerwood facility and found a work environment consistent with other Apple locations.
> The working environment was uncomfortable in other ways, according to current and former contractors. Apex managers sometimes broke up unauthorized water-cooler socializing. Several workers say their managers would get notifications if their workstations were idle for too long. "Being monitored like that is super dehumanizing and terrifying," says one former Apex mapping technician.

Apple contractors 'regularly hear confidential details' on Siri recordings
Alex Horn | Guardian | 2019
https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings

> Accidental activations led to the receipt of the most sensitive data that was sent to Apple. Although Siri is included on most Apple devices, the contractor highlighted the Apple Watch and the company's HomePod smart speaker as the most frequent sources of mistaken recordings. "The regularity of accidental triggers on the watch is incredibly high," they said. "The watch can record some snippets that will be 30 seconds – not that long but you can gather a good idea of what's going on."
> Sometimes, "you can definitely hear a doctor and patient, talking about the medical history of the patient. Or you'd hear someone, maybe with car engine background noise – you can't say definitely, but it's a drug deal … you can definitely hear it happening. And you'd hear, like, people engaging in sexual acts that are accidentally recorded on the pod or the watch."

Apple Warns Employees to Stop Leaking Information
Saturday, April 14, 2018
https://mjtsai.com/blog/2018/04/14/apple-warns-employees-to-stop-leaking-information/

> The Cupertino, California-based company said in a lengthy memo posted to its internal blog that it "caught 29 leakers," last year and noted that 12 of those were arrested. "These people not only lose their jobs, they can face extreme difficulty finding employment elsewhere," Apple added. The company declined to comment on Friday.
> Apple outlined situations in which information was leaked to the media, including a meeting earlier this year where Apple's software engineering head Craig Federighi told employees that some planned iPhone software features would be delayed. Apple also cited a yet-to-be-released software package that revealed details about the unreleased iPhone X and new Apple Watch.
> Getting fired for leaking — we all knew that happened. But this is the first I've heard of leakers being prosecuted criminally and going to jail.

Leaked recording: Inside Apple's global war on leakers: Former NSA agents, secrecy members on product teams, and a screening apparatus bigger than the TSA.
The Outline | William Turton | JUN 20 2017
theoutline.com/post/1766/leaked-recording-inside-apple-s-global-war-on-leakers

> According to the hour-long presentation, Apple's Global Security team employs an undisclosed number of investigators around the world to prevent information from reaching competitors, counterfeiters, and the press, as well as hunt down the source when leaks do occur. Some of these investigators have previously worked at U.S. intelligence agencies like the National Security Agency (NSA), law enforcement agencies like the FBI and the U.S. Secret Service, and in the U.S. military.
> The briefing, which offers a revealing window into the company's obsession with secrecy, was the first of many Apple is planning to host for employees.

The presentation starts and ends with videos, spliced with shots of Tim Cook presenting a new product at one of Apple's keynotes, that stress the primacy of secrecy at Apple. "When I see a leak in the press, for me, it's gut-wrenching," an Apple employee says in the first video. "It really makes me sick to my stomach." Another employee adds, "When you leak this information, you're letting all of us down. It's our company, the reputation of the company, the hard work of the different teams that work on this stuff."

Steve Jobs ran a notoriously secretive ship during his tenure as Apple's CEO, and in 2004 the company even unsuccessfully tried to subpoena a group of tech bloggers to unmask their sources. Cook first publicly mentioned doubling down on secrecy at a 2012 tech conference, and this presentation seems intended to reveal the results of that effort.

"This has become a big deal for Tim," Greg Joswiak, Apple's Vice President of iPod, iPhone and iOS product marketing, says in one of the videos. "Matter of fact, it should be important to literally everybody at Apple that we can't tolerate this any longer." Later, Joswiak adds that "I have faith deep in my soul that if we hire smart people they're gonna think about this, they're gonna understand this, and ultimately they're gonna do the right thing, and that's to keep their mouth shut."

To make sure of it, Apple has built an infrastructure and a team "to come after these leakers," Joswiak says, and "they're being quite effective."

She then introduces David Rice to talk about the "New Product Security" team, a part of the larger Global Security team that Rice says "is really a secrecy group, we're a little bit misnamed." Rice worked at the NSA as a Global Network Vulnerability Analyst for four years, and before that was a Special Duty Cryptologist in the U.S. Navy. He's directed the Global Security team at Apple for more than six years, according to his LinkedIn page. Hubbert also introduces Lee Freedman, who previously worked as the Chief of Computer Hacking Crimes at the U.S. Attorney's Office and as an Assistant U.S. Attorney in Brooklyn, according to LinkedIn. He joined Apple to lead Worldwide Investigations in 2011.

The presentation shifts away from China to focus on leaks coming from Apple's campuses in the U.S. In the past, Apple's U.S. employees have griped about draconian security measures, Rice says, because of the leakiness of the supply chain. "You always get this battle ... like, 'Well, why do we have to do all this security stuff when our supply chain leaks so much?'" Rice says. "I think the noise has always been high here and once the supply chain noise dropped down suddenly we realized, 'Oh crap. We have a problem here.'"Apple embeds members of a team within Global Security, called Secrecy Program Management, on some product teams to help employees keep secrets, he explains. But when sensitive information does get out, Lee Freedman's investigations team steps in to figure out what happened and who is responsible.

"So can you paint a picture of the characteristic[s] of the leakers?" Hubbert asks. "I mean, is there a common thread to what they do?"

"The common thread is they look just like you guys," Freedman says to the assembled employees. "They come to work, they don't appear any different, and they start off with the exact same motivation about 'I love Apple, I think this is a cool place to work, I wanna make it better.'"

Rice says that Apple's focus on secrecy has not translated to a culture of fear. "I think what is unique at Apple is that we don't have a Big Brother culture," Rice says. "There's nobody on my team reading emails, sitting behind you on the bus, we don't do that."

But the presentation makes working for Apple sound like working for the CIA. (At one point, Rice even refers to "blowing cover.") There are repeated references to employees drawing boundaries in their personal lives, for example. "I go through a lot of trouble not to talk about what I work on with my wife, with my teenage kids… with my friends, my family," an employee in one of the videos says. "I'm not telling you that you give up all relationships," Rice says, "but that you have a built-in relationship monitor that you're constantly using."
"Active solicitation" is just one part of secrecy at Apple, Rice says; there is also the risk of passively mentioning something. Apple employees are expected to be discreet in their own office. The hallway and the Apple lobby are referred to as "red zones," which "aren't places to talk," Rice says. The fear of accidentally "breaking secrecy" may be why some newly hired Apple employees tend to delete their Twitter accounts. Jonathan Zdziarski, a high profile security researcher, locked down his Twitter account after being hired by Apple.
"The sense we get when we talk to Apple engineers across the board is like, 'Well gosh, what if I say something in a park? Did I just break secrecy?'" Rice clarifies that the internal myth that anything not on Apple.com is confidential isn't true. Employees are free to share some things with outsiders, he says, like how "crappy [their] boss is" or their salary information, and they're free to talk to law enforcement "if the company is doing something illegal." The hard lines, he says, are around unreleased products, unreleased services, or availability of products, which Apple expects employees not to talk about with anyone who hasn't been "disclosed."
Rice urges employees to come forward if they are worried about having "broken secrecy." Nine times out of 10, when people get in trouble at Apple, he says, it's because they tried to cover up a mistake.
"Our role at NPS was created because someone spent three weeks not telling us a prototype was in a bar somewhere," Rice says in the briefing, referring to the prototype iPhone 4 left in a bar by an Apple employee that made its way to Gizmodo in 2010. That leak was so devastating to Apple that Steve Jobs personally called the editor of Gizmodo to ask for the phone back. "The crime was in the coverup."

'They'll squash you like a bug': how Silicon Valley keeps a lid on leakers
Olivia Solon Fri 16 Mar 2018 09.00 GMT
https://www.theguardian.com/technology/2018/mar/16/silicon-valley-internal-work-spying-surveillance-leakers

The public image of Silicon Valley's tech giants is all colourful bicycles, ping-pong tables, beanbags and free food, but behind the cartoonish facade is a ruthless code of secrecy. They rely on a combination of Kool-Aid, digital and physical surveillance, legal threats and restricted stock units to prevent and detect intellectual property theft and other criminal activity. However, those same tools are also used to catch employees and contractors who talk publicly, even if it's about their working conditions, misconduct or cultural challenges within the company.
While Apple's culture of secrecy, which includes making employees sign project-specific NDAs and covering unlaunched products with black cloths, has been widely reported, companies such as Google and Facebook have long put the emphasis on internal transparency.
Companies will also hire external agencies to surveil their staff. One such firm, Pinkerton, counts Google and Facebook among its clients.

> Among other services, Pinkerton offers to send investigators to coffee shops or restaurants near a company's campus to eavesdrop on employees' conversations.
> Through LinkedIn searches, the Guardian found several former Pinkerton investigators to have subsequently been hired by Facebook, Google and Apple.
> "These tools are common, widespread, intrusive and legal," said Al Gidari, consulting director of privacy at the Stanford Center for Internet and Society.
> "Companies are required to take steps to detect and deter criminal misconduct, so it's not surprising they are using the same tools to make sure employees are in compliance with their contractual obligations."

The Right to Read User E-mails
Wednesday, March 26, 2014
https://mjtsai.com/blog/2014/03/26/the-right-to-read-user-e-mails/

> Microsoft is not unique in claiming the right to read users' emails – Apple, Yahoo and Google all reserve that right as well, the Guardian has determined.
> Google's terms require the user to "acknowledge and agree that Google may access… your account information and any Content associated with that account… in a good faith belief that such access… is reasonably necessary to… protect against imminent harm to the… property… of Google". Apple "may, without liability to you, access… your Account information and Content… if we have a good faith belief that such access… is reasonably necessary to… protect the… property… of Apple".
> A few years ago, I'm nearly certain that Google accessed my Gmail account after I broke a major story about Google. A couple of weeks after the story broke my source, a Google employee, approached me at a party in person in a very inebriated state and said that they (I'm being gender neutral here) had been asked by Google if they were the source. The source denied it, but was then shown an email that proved that they were the source.
> The source had corresponded with me from a non Google email account, so the only way Google saw it was by accessing my Gmail account.
> In short, even the best privacy policy, crafted lovingly by People Who Really Care™, and agreed to under oath by every employee, doesn't actually protect your privacy. The most it can do — and even this is a stretch — is provide you some recourse if your policy should be violated. If you can prove that this happens, maybe someone will be fired or maybe you'll get financial compensation or whatever. But in the United States, even where the law says a company must *have* a privacy policy, it doesn't necessarily mean that the privacy policy is legally binding. And if it were, it would still be like any other law: it would penalize, but not prevent, misbehavior.

Did Apple snoops pose as cops in iPhone hunt? (UPDATED)
Sept. 2, 2011 By Wilson Rothman
https://www.nbcnews.com/tech/tech-news/did-apple-snoops-pose-cops-iphone-hunt-updated-flna121012

> SF Weekly previously reported that SFPD had no record of the investigation, which seemingly debunked the CNET report. If Apple investigators had simply referred to themselves as SFPD,

that would explain the absence of a report — not to mention the un-cop-like practice of offering the source money when the phone failed to turn up in his apartment.
This would all still remain in the realm of hearsay if it weren't for a piece of startling corroborative evidence: The source claiming that his home was raided, 22-year-old Sergio Calderón, said he received a phone number from one of the alleged police officers. When SF Weekly called the number, they reached a former police sergeant who is now a "senior investigator" at Apple.
The allegation of impersonating a police officer is pretty serious — SF Weekly acknowledges that in California, cop impersonation can land someone in jail for a year — and because of this, we decided to leave out the name of the accused investigator. There's probably more to this story on the way, but until charges are pressed, or at least more concrete evidence comes to light, it's all up in the air.
And so, with some nice investigative reporting, the story becomes both more outrageous and more credible at the same time. We have reached out to Apple, and will let you know if we hear any official word from the company.

Apple's Sleazy Secret Police Lose Their Leader
Ryan Tate 11/04/11 12:57AM
www.gawker.com/5856260/apples-sleazy-secret-police-lose-their-leader

Leave no fingerprints. That's the way corporate security is supposed to work. But John Theriault left big, messy ones when his Apple security agents penetrated the home of an innocent San Francisco man. Now Theriault is out of a job, and his creepy security department will probably be a lot more careful—about getting caught.
Theriault has parted ways with Apple in the wake of a scandalous San Francisco home search, 9 to 5 Mac reports. He'd been Apple's vice president of global security since 2007, after running Pfizer's crackdown on fake Viagra and after 26 years in the FBI. He apparently oversaw Apple's "Worldwide Loyalty Team," an internal secret police team known for its network of informers and ruthless, systematic pursuit of leakers.
But it was in an external operation where Theriault's crew really ran off the rails. They were exposed, via some dogged reporting by SF Weekly, for an incredibly sordid home search this past July in pursuit of an iPhone prototype that had been lost in a bar. Accompanied by three or four plainclothes San Francisco police officers, two Apple security officers searched 22-year-old Sergio Calderón's house in Bernal Heights. The officers identified themselves as police; the Apple guys did not identify themselves at all, leaving the impression they were law enforcement officers like the others. Calderón let the Apple officers in, thinking they were cops, and knowing he had no iPhone prototype. His thanks for this openness was to have his family threatened with deportation:
"One of the officers is like, 'Is everyone in this house an American citizen?' They said we were all going to get into trouble," Calderón said.
The search was never supposed to make the papers; the actual cops involved somehow kept it out of official records, to the extent that police spokesmen, when first asked about the incident, said it appeared to be a troubling case of police impersonation "that's going to need to be investigated now." There is indeed an investigation, albeit not one as straightforward as a case of six fake cops.

> Apple needn't have gotten its hands dirty, it could have made the police do its dirty work. That's how it worked with the raid on the home of Jason Chen, former editor of our sister publication Gizmodo. After Gizmodo paid for and published video of an iPhone 4 prototype that had been left in a bar, San Mateo Sheriff's deputies conducted an illegal raid of Chen's home. When San Mateo's district attorney later withdrew the warrant under which the raid had been conducted and instructed Chen get all his stuff back, Apple didn't have to deal with any blow back because it was not directly involved in the search, it simply oversaw the task force that conducted the raid. That's how it's supposed to work. If your agents do end up menacing civilians, for God's sake keep it quiet. Theriault didn't keep things quiet, at all. And we all know how Apple feels about unplanned publicity.

For lost iPhone, SFPD wants bar's surveillance video
Greg Sandoval, Declan McCullagh Sept. 25, 2011 4:00 a.m. PT
https://www.cnet.com/news/for-lost-iphone-sfpd-wants-bars-surveillance-video/#ixzz1Z0lwzTTq

> On August 31, CNET broke the news that a two-man Apple security team had gone to SFPD's Ingleside station and asked for help locating a phone that they said was lost by an unidentified Apple employee at Cava 22 sometime around Friday, July 22. They told police that the phone was priceless. Apple's security team and police officers then went to a Bernal Heights home where Apple said it had electronically tracked the handset. SFPD acknowledged assisting Apple but said a search of the home, car and computer belonging to Sergio Calderon, 22, was conducted exclusively by Apple employees.
> Calderon told SFWeekly, an alternative newspaper, that six people came to his family's house looking for the phone. He said they identified themselves as police and the Apple employees never identified themselves. He said he never would have allowed them to search his house if he knew they weren't all cops. Calderon acknowledged to police and Apple's investigators that he indeed was at Cava 22 the night the phone was lost there but denied knowing anything about its disappearance. Calderon did not respond to requests to comment for this story. Apple representative declined to comment.

Police task force oversight committee has included Apple
April 27, 2010 at 5:51 p.m. ET
www.marketwatch.com/story/apple-has-sat-on-steering-committee-for-task-force-2010-04-27

> SAN FRANCISCO (MarketWatch) -- A steering committee charged with direction and oversight of a California police task force that last week raided the home of a blogger who had published information about a lost Apple Inc. iPhone prototype has included members of several large Silicon Valley firms -- including Apple.
> The steering committee overseeing the Rapid Enforcement Allied Computer Team, or REACT, included Apple, Google Inc. Adobe Systems Inc. and others, according to the state's High Technology Crime Advisory Committee's annual report for 2008.
> The committee's report for 2009 does not detail the composition of the REACT task force steering committee. However, the Santa Clara County District Attorney's office said in a statement released Tuesday that "there is no defined membership" of the committee.

Committee meetings are open to all company representatives, according to the statement. "While our records have not shown its attendance as of late, Apple is similarly situated as other companies or entities, which have open invitations to attend."
Santa Clara County is home to Apple and numerous other technology companies. The Santa Clara County District Attorney's office is the lead agency for the REACT task force, which is composed of state and federal officers and agents.
On Friday, members of the REACT task force executed a warrant to search the home of a Gizmodo.com blogger, seizing computers and other equipment.
Gizmodo had published a report and photos detailing what appeared to be a prototype for a forthcoming model of Apple's iPhone, after it was lost in a Redwood City, Calif. bar. The blog, operated by Gawker Media LLC, later acknowledged having paid $5,000 to an unidentified individual who recovered the lost phone and sold it to them.
The REACT task force is one of several task forces operating in different regions of California, stemming from the state's High Technology and Theft Apprehension Program. Each task force is directed by a local steering committee that includes "members of the local high technology industry," according to public documents.
The REACT task force was established by an initial grant awarded in 1999, according to the High Technology Crime Advisory Committee's annual report for 2009. The task force received $2.3 million in total funding in fiscal 2009, according to the report, while conducting 102 "high-tech investigations" and making 28 arrests. Those arrests resulted in 12 convictions.
The task force also conducted 94 investigations in identity theft cases, according to the report.
Gawker has argued that the REACT task force acted in violation of California's shield law, designed to protect journalists from being forced to divulge sources, by executing the search warrant. The San Mateo County's District Attorney's office said Tuesday that it will wait on searching the machines until it determines the legality of the warrant.
The Gizmodo blogger stated in documents posted on the site that he returned home Friday evening to find his front door broken down, and REACT officers already in the process of searching through his possessions.
Gawker had earlier responded to an official request from Apple by returning the lost iPhone prototype.

Former Apple marketing manager describes company's 'controlled leaks'
AppleInsider | Jan 06, 2010
https://appleinsider.com/articles/10/01/06/former_apple_marketing_manager_describes_companys_controlled_leaks.html

As a former senior marketing manager at Apple, he said he was told to leak information in the past. He said a senior company executive would ask him to release specific information to a trusted person at a major media outlet. Martellaro claims he was asked to "idly mention" the information in a telephone conversation, and to suggest to a reporter that publishing it would be "nice." E-mail correspondence was not allowed.
"The communication is always done in person or on the phone. Never via e-mail," he said. "That's so that if there's ever any dispute about what transpired, there's no paper trail to contradict either party's version of the story. Both sides can maintain plausible deniability and simply claim a misunderstanding. That protects Apple and the publication."

The Journal's top technology commentator, Walt Mossberg, was bypassed, Martellaro alleged, to allow him to remain "above the fray." In addition, the story was leaked late Monday, after the stock market closed, so no one could suggest there was an attempt to manipulate Wall Street.
While Apple sometimes leaks information to its advantage, it also goes to great lengths to control what is publicly said, and when. Apple's tight-lipped nature was profiled last year by the New York Times, which said the company's veil of secrecy began to take shape around the release of the original Macintosh back in 1984.
One employee said that employees working on secret projects at Apple must "pass through a maze of security doors, swiping their badges again and again and finally entering a numeric code to reach their offices." Once inside the top-secret areas, employees are often monitored by surveillance cameras as they work. Those working with the most sensitive projects are allegedly instructed to "cover up devices with black cloaks when they are working on them, and turn on a red warning light when devices are unmasked so that everyone knows to be extra-careful."
Last month, one report highlighted Apple's supposed "Worldwide Loyalty Team," which are claimed to be a group of moles that spy on people and report directly to co-founder Steve Jobs and Chief Financial Officer Peter Oppenheimer. When an employee is suspected of a leak, the source claimed that they are under a "gag order" that involves the confiscation of cell phones and a total blackout of all unmonitored communication.

OverREACTing: Dissecting the Gizmodo Warrant
EFF | Matt Zimmerman | APRIL 27, 2010
www.eff.org/deeplinks/2010/04/gizmodo-search-warrant-illegal

Under California and federal law, this warrant should never have issued. First, California Penal Code Section 1524(g) provides that "[n]o warrant shall issue for any item or items described in Section 1070 of the Evidence Code." Section 1070 is California's reporter's shield provision (which has since been elevated to Article I, § 2(b) of the California Constitution). The items covered by the reporter's shield protections include unpublished information, such as "all notes, outtakes, photographs, tapes or other data of whatever sort," if that information was "obtained or prepared in gathering, receiving or processing of information for communication to the public."
The warrant explicitly authorizes the seizure of such protected materials and information, including the photographs and video taken of the iPhone prototype, as well as research regarding the Apple employee who purportedly lost the phone. This fact alone should have stopped this warrant in its tracks.
The police appear to have gone too far. The REACT team, "a partnership of 17 local, state, and federal agencies" with a "close working partnership with the high tech industry," seems to have leapt eagerly to Apple's aid before it looked at the law. Putting the presumed interests of an important local company before the rights guaranteed by law is an obvious occupational hazard for a police force charged with paying particular attention to the interests of high tech businesses.
Now that First Amendment lawyers, reporters, and others have highlighted the potential legal improprieties of this search, the task force should freeze their investigation, return Chen's property, and reconsider whether going after journalists for trying to break news about one of the Valley's most secretive (and profitable) companies is a good expenditure of taxpayer dollars.

Apple's Obsession With Secrecy Grows Stronger
New York Times | Brad Stone and Ashlee Vance | Jun 22 2009
https://www.nytimes.com/2009/06/23/technology/23apple.html?_r=2

> Few companies, indeed, are more secretive than Apple, or as punitive to those who dare violate the company's rules on keeping tight control over information. Employees have been fired for leaking news tidbits to outsiders, and the company has been known to spread disinformation about product plans to its own workers.
> "They make everyone super, super paranoid about security," said Mark Hamblin, who worked on the touch-screen technology for the iPhone and left Apple last year. "I have never seen anything else like it at another company."
> Secrecy at Apple is not just the prevailing communications strategy; it is baked into the corporate culture. Employees working on top-secret projects must pass through a maze of security doors, swiping their badges again and again and finally entering a numeric code to reach their offices, according to one former employee who worked in such areas.
> Work spaces are typically monitored by security cameras, this employee said. Some Apple workers in the most critical product-testing rooms must cover up devices with black cloaks when they are working on them, and turn on a red warning light when devices are unmasked so that everyone knows to be extra-careful, he said.
> He added: "But what most people don't understand is that Steve has always been very personal about his life. He has always kept things close to the vest since I've known him, and only confided in relatively few people."
> Apple's decision to severely limit communication with the news media, shareholders and the public is at odds with the approach taken by many other companies, which are embracing online outlets like blogs and Twitter and generally trying to be more open with shareholders and more responsive to customers.
> "They don't communicate. It's a total black box," said Gene Munster, an analyst at Piper Jaffray who has covered Apple for the last five years.

Apple: Secrecy Does Not Scale
Anil Dash | Jul 31, 2009
dashes.com/2009/07/31/apple_secrecy_does_not_scale/

> Apple is justifiably revered in the worlds of technology and culture for creating one of the most powerful brands in the world based on the combination of some key elements: Great user experience and design, and an extraordinary secrecy punctuated by surprising reveals. But the element of secrecy that's been required to maintain Apple's mystique has incurred an increasingly costly price. Apple must transform itself and leave its history of secrecy behind, not just to continue being innovative and to protect the fundamentals of its business, but because the cost of keeping these secrets has become morally and ethically untenable.
> This means that those of us who support Apple with our dollars and attention are supporting a company that chooses to operate with an **extreme and excessive layer of secrecy**, even when making reasonable business decisions. This squelching of communication about Apple's products results in customers being unhappy or uncertain of the future value of their purchases, developers being too afraid to bet their livelihoods on a platform whose fundamental

opportunities could be destroyed at any time, and suppliers being forced to inflict unreasonable or even inhumane restrictions on their employees. And that's in addition to the incredible stress that Apple employees *themselves* have had to endure, from missing Christmas to get products ready for MacWorld without even being able to tell family members why they must do so, to public-facing communications staff having to endure the misery of telling developers that their products or businesses are being terminated by fiat, without so much as an explanation.
I'm certain the web's usual contingent of soulless Randists will believe this level of suffering is somehow acceptable despite its moral cost, because The Market has made Apple a success. But there's even a financial argument: Apple spends an enormous amount of money on protecting and obfuscating normal business operations that any other company can do in the open. It's hard to estimate just how much the overhead of this extreme secrecy costs the company, but it's obviously many millions of dollars extra per year. And it will only get more expensive as large-scale realtime communications get more and more commoditized.
In contrast, Apple's employees will be too cowed to publicly respond to this post, though I know they'll see it. Partners are tired of being bullied or facing petulant sanctions for accidental disclosures of relatively innocuous bits of information. And eventually, anyone talented and independent-minded enough to participate in the kind of innovation practiced at Apple is going to chafe at being constrained in how they can express themselves.

Apple Gestapo: How Apple Hunts Down Leaks
Gizmodo | Jesus Diaz | 12/15/09
https://gizmodo.com/apple-gestapo-how-apple-hunts-down-leaks-5427058

They call themselves the Worldwide Loyalty Team. Among some employees, they are known as the Apple Gestapo, a group of moles always spying in headquarters and stores, reporting directly to Jobs and Oppenheimer. Here's how they hunt people down.
You may want to know about their Worldwide Loyalty Team," Tom told me recently in an email. I read what he had to say. It felt like a description of the Gestapo, without the torture and killing part.
Tom never lived in Nazi Germany, back in the time when the Geheime Staatspolizei had the power to get into any house or any office, at any time of the day or night, without any warrant or reason, to seize whatever or whoever they wanted in their never ending search to find enemies of the state. A place in which you had no right to privacy whatsoever. A place in which you were guilty until proven otherwise.
No, Tom never lived in Nazi Germany, nor in East Germany, nor in the Soviet Union, nor in Communist China. He lives in the United States. For sure, he has never been scared of losing his life nor the ones he loves, like thousands of millions in those countries. But he knows how it feels to be watched, to always be considered guilty of crimes against another kind of state. He knew how it felt to have no privacy whatsoever when he was working right here, in a little Californian town called Cupertino, in a legendary place located in One Infinite Loop.
Tom knew about all that pretty well, back when he was working at Apple Inc.
Of course, if Tom had never sent any sensitive information to media outlets, he would have never had the fear of being caught, only to get fired and sued into oblivion by Apple Legal. But the lack of any privacy whatsoever is something that he shared with all his fellow employees.

"Apple has these moles working everywhere, especially in departments where leaks are suspected. Management is not aware of them," he told me, "once they suspect a leak, the special forces—as we call them—will walk in the office at any hour, especially in the mornings. They will contact whoever was the most senior manager in the building, and ask them to coordinate the operation."

The operation, as Tom calls it, is not anything special. It is not one of a kind event. It's just a normal practice, and the process is pretty simple: The manager will instruct all employees to stay at their desks, telling them what to do and what to expect at any given time. The Apple Gestapo never handles the communication. They are there, present, supervising the supervisors, making sure everything goes as planned.

All cellphones are then taken. Usually, they collect them all at the same time, which means that the process could take a long time. If you need to contact the exterior during the time your cellphone is under examination, you will have to ask for permission, and your call will be monitored.

They don't ask for cameras because there are no cameras at Apple: Employees are not allowed to get into the campus with them. If the cellphone is an iPhone, it gets backed up onto a laptop. "In fact, at the beginning they used to say that the iPhones were really their property, since Apple gave every employee a free iPhone," he points out. All the employees are asked to unlock and disable any locking features in their cellphones, and then the special forces will proceed to check them for recent activity.

They back up everything and go through all the other phones' text messages and pictures. If you have porn in your phone, they will see it. If you have text messages to your spouse, lover, or Tiger Woods, they will see them, too. Just like that. No privacy, no limits.

While all this is happening, the employees are ordered to activate the screensaver on their computers, so the special forces are sure there are no chats happening between employees or with the exterior. They are told not to speak, text or call one other when the lockdown is happening: "It is like a gag order, and if the employee does not want to participate, they are basically asked to leave and never come back."

Of course, all this is voluntary. Management recommends that you relinquish your phones. If you don't do it they will fire you, or they will investigate why you didn't want to give them your cellphone. Simultaneously, everyone is asked to sign NDA's during the investigations, even though they already signed Apple NDAs to work there.

"I was at several events. When they find what they are looking for—which they usually do—the person is asked to stay until the end of the business day. Then he is asked to leave the premises quietly, escorted by security," Tom says. While he's there, the special forces hang around, watching. "There is a lot that goes behind doors that I don't really know about. I do know, however, that they really interrogate people that are serious suspects, intimidating them by threatening to sue."

There is no way to know how often this happens, however, as everything is handled very quietly. The same Worldwide Loyalty Team does many other things to keep everyone in check, from searching out the email history of every employee—which is also a normal practice in other corporations and government agencies—to seeding fake images to catch potential leaks and diffuse the hype about some product introductions.

As Tom was describing all this, my mind was getting back to all I've read about Steve Jobs and Apple, back when he was El Capitán of the brave group of free pirates who created the

Macintosh. The Mac was a secret project too, but there was no secret police making sure there were no leaks. After a hard day of work, all the Mac team sometimes played on the beaches of California, careless and happy, confident that this new revolutionary computer would change the world, one desktop at a time. All of them shared information, there were no seeeecrets, and that's why they came up with an "insanely great" computer, as Steve Jobs himself used to refer to it.
And while I understand that secrecy is paramount to success in today's extremely competitive market—hello, dear marketdrones—now I look at this story on the Worldwide Loyalty Team, and it makes me realize how much Apple has changed. From a happy hippie company, to a company that does KGB-style lockdowns and Gestapo interrogations that end in suicides.
I wonder if the special forces have ever chased anyone through the Infinite Loop campus, dressed in their full 1984 regalia.
I wouldn't be surprised.

Apple Privacy/Surveillance in Lawsuits

Lopez et al v Apple, Inc (2021)

- *Wire Tapping; Privacy; Breach of Contract*
- https://www.reuters.com/technology/apple-must-face-siri-voice-assistant-privacy-lawsuit-us-judge-2021-09-02/
- https://www.classaction.org/media/lopez-et-al-v-apple-inc.pdf

U.S. District Judge Jeffrey White said the plaintiffs could try to prove Siri routinely recorded their private conversations because of "accidental activations," and that Apple disclosed these conversations to third parties, such as advertisers.
Voice assistants typically react when mobile device owners use "hot words" such as "Hey, Siri." One Siri user said his private discussions with his doctor about a "brand name surgical treatment" caused him to receive targeted ads for that treatment, while two others said their discussions about Air Jordan sneakers, Pit Viper sunglasses and "Olive Garden" caused them to receive ads for those products.
"Apple faults plaintiffs for not alleging the contents of their communications, but the private setting alone is enough to show a reasonable expectation of privacy," White wrote.
The Oakland, California-based judge said the plaintiffs may pursue claims that Apple violated the federal Wiretap Act and California privacy law, and committed breach of contract. He dismissed an unfair competition claim.

Apple Inc v Williams (2020)

- *Breach of Contract; Breach of Loyalty*
- https://www.engadget.com/2019-12-10-apple-lawsuit-snooped-text-messages.html
- https://finance.yahoo.com/news/nuvia-exec-sued-apple-says-181807641.html
- https://www.semiaccurate.com/assets/uploads/2019/12/2019.08.07-Apple-v.-Williams-Complaint.pdf

But in that filing, it's clear that Apple reviewed Williams' texts and had access to his phone records. The lawsuit shares a text exchange that Williams and a fellow Apple engineer had in October 2015, and it details the frequency and length of calls Williams had with NuVia co-founders during business hours while he was employed at Apple.

Williams calls this a "stunning and disquieting invasion of privacy." Apple, like most Big Tech companies, has promised to protect users' privacy, so allegations it dug through texts and call records aren't a good look. Though, we don't know if the exchanges Apple detailed were from a company phone. If the texts and calls were made on an Apple-issued device, it's not surprising that Apple had access to those records -- but it's still a bit unsettling.

D. Williams Starts a Competing Venture with Related Technology on Apple's Time.

27. Notwithstanding his contractual obligations not to compete with Apple while working for Apple, Williams surreptitiously spent years contemplating a competing business. As early as 2015, Williams began text messaging certain colleagues about starting a business to develop computer chips for servers. The text messages evince that Williams's new venture would build technology directly related to Apple business and products. For instance, on October 5, 2015, Williams exchanged messages with a fellow Apple engineer:

> GW: Well. The server mkt is ripe for a new player. And a new supercomputer too
>
> [. . .]
>
> GW: Crap a few extra billion in a good server. Nice business
>
> AS: no one has done the server market well
>
> GW: And a game console. Another few billion.
>
> [. . .]
>
> AS: yeah just trying to think of who would acquire a server business at ridiculous multiples
>
> GW: ***Crazy thing Apple needs the software***

28. On October 17, 2015, Williams messaged another Apple engineer, describing the

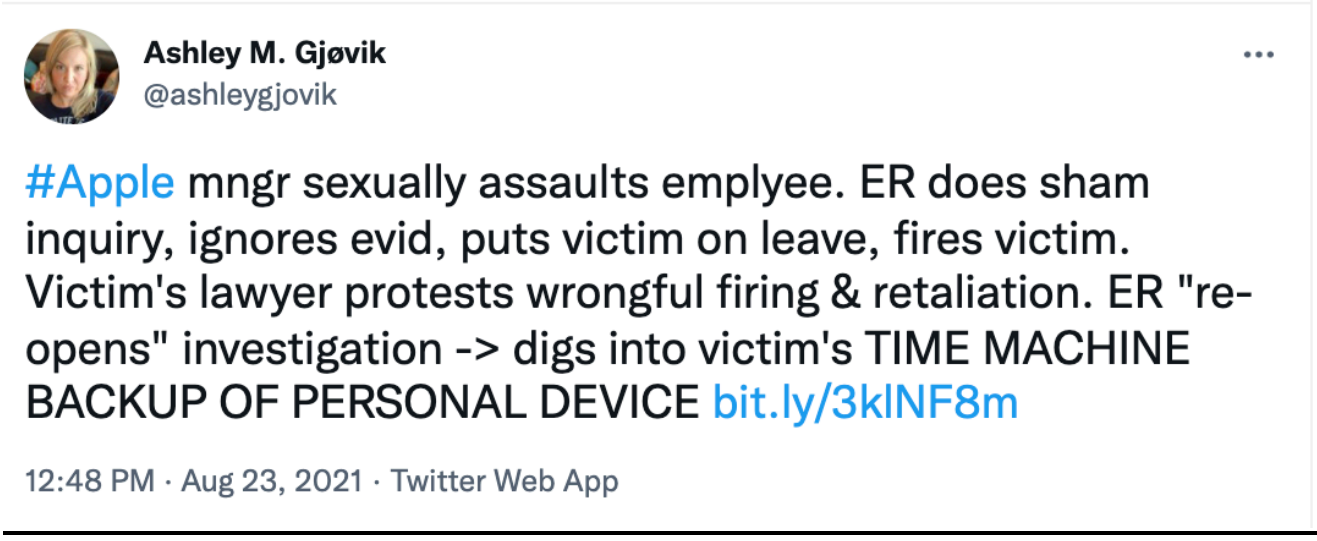
---

Richardson v Apple, Inc (2012)

- *Retaliation; Wrongful Termination; IIED*
- https://docs.justia.com/cases/federal/district-courts/california/caedce/2:2012cv02032/242428/1

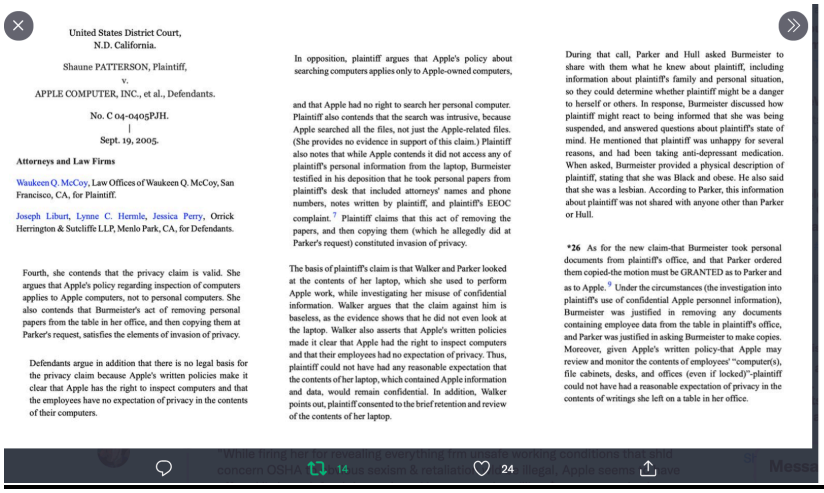
21. On or about April 16, 2012, corporate counsel for APPLE, Kwang Kim sent PLAINTIFF's counsel a letter stating that APPLE would not be terminating PLAINTIFF as originally planned, but would instead keep him on paid suspension while APPLE continued its investigation.

22. Sometime on or around APPLE's April 16, 2012 letter, APPLE "re-opened" its investigation of the February 9, 2012 incident. However, instead of interviewing additional witnesses or obtaining other relevant evidence to that evening, APPLE turned its investigation to the contents of PLAINTIFF's Time Machine backup of his personal iPhone and the private information contained therein. APPLE made no such investigation into MS. HESS-BREWER's personal information.



Patterson v Apple Computer (2005)

- *Racal Discrimination; Harassment; Sexual Orientation Discrimination; Retaliation; Defamation; Invasion of Privacy; Wrongful Termination*
- http://ca.findacase.com/research/wfrmDocViewer.aspx/xq/fac.20050919_0000386.NCA.htm/qx
- https://www.casemine.com/judgement/us/59146c61add7b0493430f019



United States District Court,
N.D. California.

Shaune PATTERSON, Plaintiff,
v.
APPLE COMPUTER, INC., et al., Defendants.

No. C 04-0405PJH.
Sept. 19, 2005.

Attorneys and Law Firms

Waukeen Q. McCoy, Law Offices of Waukeen Q. McCoy, San Francisco, CA, for Plaintiff.

Joseph Liburt, Lynne C. Hermle, Jessica Perry, Orrick Herrington & Sutcliffe LLP, Menlo Park, CA, for Defendants.

Fourth, she contends that the privacy claim is valid. She argues that Apple's policy regarding inspection of computers applies to Apple computers, not to personal computers. She also contends that Burmeister's act of removing personal papers from the table in her office, and then copying them at Parker's request, satisfies the elements of invasion of privacy.

Defendants argue in addition that there is no legal basis for the privacy claim because Apple's written policies make it clear that Apple has the right to inspect computers and that the employees have no expectation of privacy in the contents of their computers.

In opposition, plaintiff argues that Apple's policy about searching computers applies only to Apple-owned computers,

and that Apple had no right to search her personal computer. Plaintiff also contends that the search was intrusive, because Apple searched all the files, not just the Apple-related files. (She provides no evidence in support of this claim.) Plaintiff also notes that while Apple contends it did not access any of plaintiff's personal information from the laptop, Burmeister testified in his deposition that he took personal papers from plaintiff's desk that included attorneys' names and phone numbers, notes written by plaintiff, and plaintiff's EEOC complaint.[7] Plaintiff claims that this act of removing the papers, and then copying them (which he allegedly did at Parker's request) constituted invasion of privacy.

The basis of plaintiff's claim is that Walker and Parker looked at the contents of her laptop, which she used to perform Apple work, while investigating her misuse of confidential information. Walker argues that the claim against him is baseless, as the evidence shows that he did not even look at the laptop. Walker also asserts that Apple's written policies made it clear that Apple had the right to inspect computers and that their employees had no expectation of privacy. Thus, plaintiff could not have had any reasonable expectation that the contents of her laptop, which contained Apple information and data, would remain confidential. In addition, Walker points out, plaintiff consented to the brief retention and review of the contents of her laptop.

During that call, Parker and Hull asked Burmeister to share with them what he knew about plaintiff, including information about plaintiff's family and personal situation, so they could determine whether plaintiff might be a danger to herself or others. In response, Burmeister discussed how plaintiff might react to being informed that she was being suspended, and answered questions about plaintiff's state of mind. He mentioned that plaintiff was unhappy for several reasons, and had been taking anti-depressant medication. When asked, Burmeister provided a physical description of plaintiff, stating that she was Black and obese. He also said that she was a lesbian. According to Parker, this information about plaintiff was not shared with anyone other than Parker or Hull.

*26 As for the new claim-that Burmeister took personal documents from plaintiff's office, and that Parker ordered them copied-the motion must be GRANTED as to Parker and as to Apple.[9] Under the circumstances (the investigation into plaintiff's use of confidential Apple personnel information), Burmeister was justified in removing any documents containing employee data from the table in plaintiff's office, and Parker was justified in asking Burmeister to make copies. Moreover, given Apple's written policy-that Apple may review and monitor the contents of employees' "computer(s), file cabinets, desks, and offices (even if locked)"-plaintiff could not have had a reasonable expectation of privacy in the contents of writings she left on a table in her office.

Ashley M. Gjøvik
@ashleygjovik

She complained that following speaking up w/ concerns, #Apple employee retaliations went through her personal computer & personal documents (including her EEOC complaint & notes w/ her attorneys) & made copies. Apple's response: "Apple employees have no expectation of privacy."

3:24 PM · Aug 28, 2021 · Twitter Web App

View Tweet activity

9 Retweets **5** Quote Tweets **24** Likes

Ashley M. Gjøvik
@ashleygjovik

Thinking abt the Patterson case where #Apple made copies of her EEOC complaint & notes w/ lawyers. Told the court it's ok, she has no privacy.
Why wouldn't Apple have been going through my iCloud folders/emails, & reading my filings, notes, legal strategy?

Ashley M. Gjøvik @ashleygjovik · Aug 28
She complained that following speaking up w/ concerns, #Apple employee retaliations went through her personal computer & personal documents (including her EEOC complaint & notes w/ her attorneys) & made copies. Apple's response: "Apple employees have no expectation of privacy."
Show this thread

United States District Court,
N.D. California.

Shaune PATTERSON, Plaintiff,
v.
APPLE COMPUTER, INC., et al., Defendants.

No. C 04-0405PJH.
Sept. 19, 2005.

Attorneys and Law Firms

Waukeen Q. McCoy, Law Offices of Waukeen Q. McCoy, San Francisco, CA, for Plaintiff.

Joseph Liburt, Lynne C. Hermle, Jessica Perry, Orrick Herrington & Sutcliffe LLP, Menlo Park, CA, for Defendants.

Fourth, she contends that the privacy claim is valid. She argues that Apple's policy regarding inspection of computers applies to Apple computers, not to personal computers. She also contends that Burmeister's act of removing personal papers from the table in her office, and then copying them at Parker's request, satisfies the elements of invasion of privacy.

Defendants argue in addition that there is no legal basis for the privacy claim because Apple's written policies make it clear that Apple has the right to inspect computers and that the employees have no expectation of privacy in the contents of their computers.

In opposition, plaintiff argues that Apple's policy about searching computers applies only to Apple-owned computers,

and that Apple had no right to search her personal computer. Plaintiff also contends that the search was intrusive, because Apple searched all the files, not just the Apple-related files. (She provides no evidence in support of this claim.) Plaintiff also notes that while Apple contends it did not access any of plaintiff's personal information from the laptop, Burmeister testified in his deposition that he took personal papers from plaintiff's desk that included attorneys' names and phone numbers, notes written by plaintiff, and plaintiff's EEOC complaint.[7] Plaintiff claims that this act of removing the papers, and then copying them (which he allegedly did at Parker's request) constituted invasion of privacy.

The basis of plaintiff's claim is that Walker and Parker looked at the contents of her laptop, which she used to perform Apple work, while investigating her misuse of confidential information. Walker argues that the claim against him is baseless, as the evidence shows that he did not even look at the laptop. Walker also asserts that Apple's written policies made it clear that Apple had the right to inspect computers and that their employees had no expectation of privacy. Thus, plaintiff could not have had any reasonable expectation that the contents of her laptop, which contained Apple information and data, would remain confidential. In addition, Walker points out, plaintiff consented to the brief retention and review of the contents of her laptop.

During that call, Parker and Hull asked Burmeister to share with them what he knew about plaintiff, including information about plaintiff's family and personal situation, so they could determine whether plaintiff might be a danger to herself or others. In response, Burmeister discussed how plaintiff might react to being informed that she was being suspended, and answered questions about plaintiff's state of mind. He mentioned that plaintiff was unhappy for several reasons, and had been taking anti-depressant medication. When asked, Burmeister provided a physical description of plaintiff, stating that she was Black and obese. He also said that she was a lesbian. According to Parker, this information about plaintiff was not shared with anyone other than Parker or Hull.

*26 As for the new claim-that Burmeister took personal documents from plaintiff's office, and that Parker ordered them copied-the motion must be GRANTED as to Parker and as to Apple.[9] Under the circumstances (the investigation into plaintiff's use of confidential Apple personnel information), Burmeister was justified in removing any documents containing employee data from the table in plaintiff's office, and Parker was justified in asking Burmeister to make copies. Moreover, given Apple's written policy-that Apple may review and monitor the contents of employees' "computer(s), file cabinets, desks, and offices (even if locked)"-plaintiff could not have had a reasonable expectation of privacy in the contents of writings she left on a table in her office.

1:16 PM · Sep 9, 2021 · Twitter Web App

APPENDIX: Full Workplace Searches and Privacy Policy

Workplace Searches and Privacy
https://people.apple.com/US/en/subtopic/845
5/4/21, 9:42 AM

Workplace Searches and Privacy
In order to protect Apple confidential and sensitive information and maintain the security and integrity of our networks and equipment, any use of Apple property, as well as use of your personal devices for Apple business or for accessing Apple networks, is subject to this policy.

Use of Apple systems and data
All Apple facilities, furnishings, supplies, equipment, networks, and electronic systems (such as internet and intranet access, voicemail, email, instant messaging, and collaboration tools) are company property and are provided to conduct Apple business. Personal use is permitted as long as such use is reasonable and doesn't interfere with normal business activities. It must also not affect your performance, violate Apple policies and practices, or applicable local laws.
Generally, you should use Apple equipment to conduct Apple business. If you use your personal property to conduct Apple business (such as computers, data storage devices, mobile devices, and so on), or to access Apple networks, you must act in accordance with Apple policies. In addition, your property may be subject to search and the Apple-related content may be removed.

Workplace searches
Only in cases where allowed under local law, Apple may:

- Access, search, monitor, archive, and delete Apple data stored on all of its property, as well as non-Apple property, if used for Apple business or if used for accessing Apple data, servers, or networks. This includes all data and messages sent, accessed, viewed, or stored (including those from iCloud, Messages, or other personal accounts) using Apple equipment, networks, or systems.
- Conduct physical, video, or electronic surveillance, search your workspace such as file cabinets, desks, and offices (even if locked), review phone records, or search any non-Apple property (such as backpacks, purses) on company premises.

This means that you have no expectation of privacy when using your or someone else's personal devices for Apple business, when using Apple systems or networks, or when on Apple premises.
The search or removal of Apple-related content on a device will be determined on a case-by-case basis when there is a business need and subject to local approval processes. Refusing to permit a search or removal of Apple-related content may result in disciplinary action up to and including termination of employment.
If you visit the premises of current or potential customers, clients, suppliers, or vendors, you may be subject to their respective search policies and procedures. Before providing access to Apple materials, contact your manager or Global Security.

Information disclosure
If information discovered during any search indicates possible unlawful behavior, Apple may disclose that information to law enforcement officials **without notice.**