Information Security in the Courts

Emile J. Katz*

ABSTRACT

Devices with recording capabilities have become pervasive in modern life. That pervasiveness becomes concerning in areas such as Judicial chambers, where confidentiality is particularly important. Recording devices have the capability to breach that confidentiality, opening the door to dire consequences. Although courts recognize the need for confidentiality, judicial policy guides have not addressed the dangers posed by common devices with recording capabilities. The failure to address those dangers is a significant oversight, and this Article proposes one remedy to ensure information security in Judicial chambers.

Table of Contents

I. INTRODUCTION

Technological convenience has been purchased at the price of decreased privacy, a phenomenon that gives rise to concerning ramifications. Voice recognition software has become part of everyday life, but, as a result, private conversations that many individuals deem

*J.D., University of California, Berkeley School of Law. Currently a judicial law clerk, the author served as a paratrooper and sniper in the Israel Defense Forces from 2015–2017. The views expressed herein are solely the views of the author and do not represent the views of any court or judge. I would like to thank Nick Martiniano for his editorial assistance as well as Lila Englander, Itamar Vazina, Ori Hingel, and Gal Ziperfal for providing inspiration.

private have been recorded and listened to[1] and will likely continue to be.[2] When companies like Apple, Amazon, and Google listen to and record individuals in an everyday setting, it violates individuals' privacy, but the stakes are relatively low on average.[3] In cases where eavesdropping leads to a violation of privacy, statutes such as the Electronic Communications Privacy Act (ECPA)[4] provide multiple remedies. Individuals can pursue a private cause of action against electronic eavesdroppers.[5] Alternatively, eavesdroppers may be criminally prosecuted.[6] Such remedies are necessary because not every surreptitiously recorded communication is a low-stakes matter. However, not every violation can be remedied by the ECPA. There are certain situations where the stakes are so high that appropriate caution requires the removal of technology capable of recording from the vicinity altogether.

---

1. *See* Alex Hern, *Apple Contractors "Regularly Hear Confidential Details" on Siri Recordings*, THE GUARDIAN (July 26, 2019, 12:34 PM), https://bit.ly/3Ajdxcq ("Apple says the data 'is used to help Siri and dictation . . . understand you better and recognise [sic] what you say.' . . . A whistleblower working for the firm, who asked to remain anonymous due to fears over their job, expressed concerns about this lack of disclosure, particularly given the frequency with which accidental activations pick up extremely sensitive personal information."); Nick Parker, *Alexa, Stop Being a Perv: Outrage as Amazon's Alexa Listens to Brits Having Sex, Rowing, Swearing and Sharing Medical News*, THE SUN (July 29, 2019, 10:31 PM), https://bit.ly/2SJBZ5O ("Amazon staff listen to a proportion of the recordings in order to monitor and improve the system. . . . [one staff member reported] '[w]e were told to focus on Alexa commands but it was impossible not to hear other things going on.'"); Marc Weber Tobias, *Did iPhone Customers Consent To Siri Eavesdropping On Their Conversations?*, FORBES (June 8, 2020, 11:05 AM). https://bit.ly/3gkXdQa ("If the checkbox 'Allow Siri when locked' is selected, it really means that Siri can listen at any time, with or without any interaction from the phone's owner."); *see also* Jonathan Stempel, *Apple Must Face Siri Voice Assistant Privacy Lawsuit -U.S. Judge*, REUTERS (Sept. 2, 2021, 1:20 PM), https://reut.rs/3ExTUQ3.

2. Grant Clauser, *Amazon's Alexa Never Stops Listening to You. Should You Worry?*, N.Y. TIMES (Aug. 8, 2019) https://nyti.ms/36ai4zU (explaining that the data collection helps these devices improve their service and make more personalized marketing suggestions).

3. This assertion is not to suggest that individual privacy interests are unimportant. Rather, individual privacy interests simply do not usually raise critical issues of public order and safety.

4. *See* Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1848, (codified as amended at 18 U.S.C. §§ 2510–2523).

5. *See* 18 U.S.C. § 2520(a) (providing that "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate").

6. *See* 18 U.S.C. § 2511(1) (imposing criminal liability on "any person who—(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . ").

II. BACKGROUND

Judicial chambers are one such place where an abundance of caution is warranted.[7] Discussions that take place in judicial chambers among a judge and her employees are of a highly confidential nature.[8] Although the ECPA applies to recording such information, the harm that results from such information being disseminated may be beyond the ECPA's statutory ability to remedy.[9] Despite the potential for irreparable harm, seemingly no efforts have been undertaken to ensure that those communications are kept private against encroachment by technology companies whose devices are constantly recording. For example, the federal *Code of Conduct for Judicial Employees*[10] and *Code of Conduct for United States Judges*[11] make no recommendations regarding how to keep chamber conversations private from surreptitious recording. The lack of recommendations is more surprising when considering the *Code of Conduct for Judicial Employees*'s heavy emphasis on confidentiality.[12] And although the Committee on Codes of Conduct[13] issued an advisory opinion on the potential confidentiality concerns inherent in social media

7. This Article is limited to discussing surreptitious recording in judicial chambers, but much of the reasoning here could apply to other legal settings, such as law offices. In fact, the Model Rules of Professional Conduct may mandate by implication that attorneys remove all possible recording devices from their offices. Model Rule of Professional Conduct 1.6 states that "(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b)." and also that "(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." MODEL RULES OF PRO. CONDUCT r. 1.6 (AM. BAR ASS'N 1983). In order to prevent inadvertent disclosure, it may well be necessary to remove any technological device capable of recording from a law office while "information relating to the representation of a client" is being discussed.

8. *See* FEDERAL JUDICIAL CENTER, MAINTAINING THE PUBLIC TRUST: ETHICS FOR FEDERAL JUDICIAL LAW CLERKS 5 (4th ed. 2013) ("[T]he term [confidential information] generally includes any information [clerks] receive through [their] clerkship that is not part of the public record. . . . [Clerks] have a *strict obligation* to keep this information confidential, unless [their] judge specifically authorizes [them] to disclose it.").

9. Violators can be prosecuted under the ECPA, but the ECPA is meant to deter, and once confidential information is leaked, its confidentiality is gone forever. Additionally, violations of the ECPA may never even be detected. Therefore, it is necessary for judges to proactively act to protect their private communications.

10. *See generally* CODE OF CONDUCT FOR JUDICIAL EMPLOYEES (2019), https://bit.ly/3jA6A0D (containing no content on preventing technological interception).

11. *See generally*, CODE OF CONDUCT FOR UNITED STATES JUDGES (2019), https://bit.ly/2Tsa3DN (containing no content on preventing technological interception).

12. *See* CODE OF CONDUCT FOR JUDICIAL EMPLOYEES, *supra* note 10, at Canon 3(D).

13. The Committee on Codes of Conduct is part of the Judicial Conference of the United States and publishes "formal advisory opinions on ethical issues that are frequently raised or have broad application." *Ethics Policies*, UNITED STATES CTS., https://bit.ly/3ybHZTZ (last visited Sept. 4, 2021).

use by judges and judicial employees, the committee has yet to recognize that recording by technology companies may raise even greater confidentiality concerns.[14] The Joint Technology Committee[15] has released a report entitled *Cybersecurity Basics for Courts*[16] that covers some methods for protecting sensitive court information from cybersecurity threats. However, despite recognizing the likelihood that courts will increasingly face cybersecurity threats,[17] the report provides no guidance on avoiding such attacks when carried out by means of surreptitious recording.

Several scenarios illuminate the need to adopt a policy to prevent recording. Recently, reports revealed the Department of Justice's attempt to obtain secret subpoenas requiring Apple to turn over the private "phone records of House Intelligence Committee officials."[18] If the executive branch can invade the privacy of legislative officials, there is no reason to believe that private conversations within judicial chambers are immune from similar efforts. In our government system, the courts are meant to serve as a check on the executive and legislative branches.[19] Such checks and balances were put in place to protect the rights of individual citizens from government overreach.[20] Yet, if the Executive or Legislative Branch is able to acquire confidential communications that occur in judicial chambers, those branches could obtain a strategic advantage when litigating against private individuals, thus undermining the judicial branch's ability to serve as an effective check against those other branches.

14. *See* COMMITTEE ON CODES OF CONDUCT, ADVISORY OPINION NO. 112: USE OF ELECTRONIC SOCIAL MEDIA BY JUDGES AND JUDICIAL EMPLOYEES, PUBLISHED ADVISORY OPINIONS 224–29 (2017), https://bit.ly/3wbxtdY.

15. The Joint Technology Committee was established by The Conference for State Court Administrators, the National Association for Court Management, and The National Center for State Courts. *See Joint Technology Committee*, NAT'L CTR. FOR ST. CTS., https://bit.ly/3ydZgf9 (last visited Sept. 4, 2021).

16. JOINT TECHNOLOGY COMMITTEE, JTC RESOURCE BULLETIN: CYBERSECURITY BASICS FOR COURTS (2019), https://bit.ly/3h8F3So.

17. *See id.* at 2 ("Courts may believe they are unlikely to be victims of cybersecurity incidents because they don't manage large databases of credit card information. However, threats are real and increasing.").

18. *See* Sadie Gurman & Siobhan Hughes, *Apple Subpoenas From DOJ Prompt Internal Review, Calls for William Barr, Jeff Sessions to Testify*, WALL ST. J., (June 11, 2021, 10:02 PM), https://on.wsj.com/3dAmtjK; Katie Benner, et al., *Hunting Leaks, Trump Officials Focused on Democrats in Congress*, N.Y. TIMES (June 10, 2021), https://nyti.ms/3dzfBDt; Sadie Gurman, *After Apple Subpoenas, Justice Department Rethinks Policies on Getting Lawmakers' Records*, WALL ST. J, (June 14, 2021, 6:50 PM), https://on.wsj.com/3f8BbiH.

19. *See* ALEXANDER HAMILTON, THE FEDERALIST NO. 78 (1788).

20. *See id.*

Several hypothetical situations further demonstrate the need for judges to take proactive steps to prevent audio surveillance. For example, imagine a situation where law enforcement officers apply for a warrant permitting a raid of a technology company's offices after obtaining probable cause that the company has engaged in illegal conduct. While reviewing the warrant application, the issuing judge mentions the technology company by name. The judge's chambers uses that company's technology and the use of the company's name inadvertently activates the listening function of one of the company's recording devices. The company is alerted to the upcoming search and destroys evidence of criminal conduct before the warrant is served.[21]

In another hypothetical, a technology company is sued. An intrepid company employee discovers that the judge herself is a subscriber to the company's technology services. The employee then uses those services to listen to conversations that occur within the judge's chambers and learns how the judge is thinking about the case. The employee turns over a transcript of the confidential conversation to the company's legal department, which then uses that information to perfectly tailor their legal motions and litigation strategy to address the judge's concerns.[22] By doing so, the company has obtained an unfair strategic advantage over the plaintiff suing it.

Alternatively, imagine that a victim files for a protective order against an abusive partner after leaving their relationship. The protective order is granted, and the abusive partner is enraged. The abuser happens to work for a technology company whose products include recording devices. Hoping to get back at the judge, the abuser checks to see if the judge subscribes to the company's services and discovers that the judge does. The abuser listens to conversations and, in the process, learns his victim's new address. The abuser then attacks the victim. Even if an abuser does not work at a technology company, they may have friends who do and who would be willing to help them.

Finally, organized crime elements might solicit, or use threats to obtain, assistance from technology company employees to listen in and

21. Undoubtedly, if a company destroyed evidence after surreptitiously recording a chambers conversation, it would be violating several additional laws. However, the violations may never be discovered, and even if the violations are discovered, it may be too late to recover evidence of the original crime.

22. These concerns are not limited to arguing the merits but might extend to procedural strategy as well. For example, if the judge is particularly ill-inclined to rule for the company, the company could seek removal to another court or a change of venue so that the case would be heard by another judge.

learn where key witnesses are located. Organized crime elements might then use that information to threaten, or even silence, key witnesses. A technology company employee might even overhear a warrant application being granted for a raid on an organized crime organization and decide to sell that information to the organization, thereby endangering law enforcement officers and their investigation. All of these issues are heightened in the case of a Foreign Intelligence Surveillance Act ("FISA")[23] court because leaked information presented to a FISA court can directly harm national security and key intelligence assets.[24]

One can hope that employees or contractors of these companies are honest and upstanding citizens and that they would not intentionally violate the confidentiality of judicial chambers. However, the risks and dangers if such a situation were ever to occur are too great to leave to hope. These scenarios may seem far-fetched. And yet, from a technological standpoint, nothing is stopping these scenarios from coming to fruition. Furthermore, none of the above scenarios even take into account the possibility that companies with recording abilities might themselves be hacked and that those hackers might obtain the recorded information. The possibility of a hacker using these recording capabilities is perhaps more likely and more worrisome because of hackers' near-certain improper motives.

Due to similar information safety concerns, the Israel Defense Forces (IDF) has adopted practices to protect sensitive information.[25] Whenever commanders want to discuss the details of an upcoming operation, they require every member of the team to surrender their cell phone and place them into a box, which was placed outside of the briefing room. This practice was a response to reports that Hamas, a Gazan terror organization, had the ability to surreptitiously access certain cell phone microphones and

23. *See About the Foreign Intelligence Surveillance Court*, UNITED STATES FOREIGN INTEL. SURVEILLANCE CT. ("The Foreign Intelligence Surveillance Court . . . entertains applications submitted by the United States Government for approval of electronic surveillance, physical search, and other investigative actions for foreign intelligence purposes. Most of the Court's work is conducted ex parte as required by statute, and due to the need to protect classified national security information."), https://bit.ly/2UjsvOS (last visited Sept. 4, 2021).

24. Hopefully, policies to prevent secret recording are already in place in FISA courts. However, considerable research on the subject has not exposed anything to suggest that such policies exist.

25. No official IDF manual explicates this practice. However, through virtue of service as an IDF paratrooper, the Author has personally observed that this practice was adopted.

thereby listen in on confidential information which could place IDF forces in danger.[26]

III. PROPOSAL

To combat information safety concerns, this Article proposes that the Judicial Conference of the United States (and similar organizations across the world) adopt an official policy similar to the one employed by the IDF. Namely, judges and judicial employees should leave their cell phones and other technology capable of recording conversations outside the judicial chambers. If the judge has a reception area or front desk, such technology could be left there, preferably in an enclosed box, away from the interior of chambers where confidential conversations may occur. Pursuant to such a policy, devices similar to Amazon's Echo, Google's Nest, or Apple's Homepod would be completely banned from all chambers, given that such devices are designed to record. Admittedly, such a policy may reduce the convenience of listening to music in chambers or using voice activation to send messages or search the web, but the tradeoff in increased judicial privacy is worth the inconvenience. Companies' promises not to record are not sufficient to protect the judiciary's integrity. Equally insufficient would be to allow such devices in chambers upon a promise that the recording feature is turned off. Keeping recording technology out of judicial chambers altogether is a best practice and should become a requirement.

As a final note, and an additional inducement to adopt the proposed policy, if the recommendations in this Article are adopted, the implementation of this policy may have an additional benefit completely unrelated to improved information security: work efficiency. Without the distractions of phones and other devices, judges and judicial employees will likely have less access to social media throughout the day. There has been a wealth of research demonstrating that social media use is correlated

26. *See* Ruth Eglash, *Israel Says Hamas Hacked Facebook Accounts, Cellphones of Army Recruits*, WASH. POST (Jan. 11, 2017), https://wapo.st/3y0DNpC (discussing Gazan hacking of Israeli soldier's phones); Yaniv Kubovich, *Hamas Hacked Hundreds of Israeli Soldiers' Phones Using Fake Social Media Accounts,* HAARETZ (Feb. 16, 2020), https://bit.ly/2UAsab9 (describing Hamas hacking of Israeli phones). However, hacking as a form of military surveillance is not exclusive to Hamas. *See* Thomas Brewster, *Facebook Warning: U.S. Military Targeted By Iranian Hackers Posing As Attractive Women*, FORBES (July 15, 2021, 1:00PM), https://bit.ly/37lLQCF; Giuliano J. de Leon, *New Way to Identify if Your Android or iPhone's Camera and Mic Is Secretly Used... Here's What You Need to Do*, TECH TIMES (Oct. 4, 2020, 7:10 AM), https://bit.ly/2V0qEz5; Thomas Germain, *How to Protect Yourself From Camera and Microphone Hacking*, CONSUMER REPS. (July 16, 2019), https://bit.ly/3wbrZQr; Brandon Jones, *Can Hackers Access Your Phone's Camera and Microphone?*, DFNDR BLOG (July 25, 2016), https://bit.ly/3wczRkz.

with decreased task efficiency and decreased well-being.[27] Therefore, even if a judicial chambers never faces a situation where chambers conversations would be recorded, the policies advocated for are still beneficial. Given the serious risks involved in any chance of judicial communications being secretly recorded and the benefits from keeping recording technology out of chambers, organizations such as the Judicial Conference of the United States should adopt official policies addressing this issue and recommend that all recording technology be kept out of chambers.

In most instances, an office phone should be sufficient if someone needs to contact a judge or judicial employee. However, some judges and judicial employees may need their cellphones in chambers to stay in touch with family, especially individuals with young children. In those cases, as an alternative, judges might consider adopting a policy of allowing cell phones so long as they are removed when orally discussing any judicial activity.

IV. CONCLUSION

The work of the judiciary in the United States has far reaching ramifications for both the public at large and individual litigants. Part of the reason we trust the courts with so much power is that we believe in the adversarial system of adjudication where litigants play—at least paradigmatically—on an informationally level playing field. However, if parties can obtain an informational advantage by listening in on chambers conversations that are meant to be private, the integrity of the system will quickly fail. And beyond the issues for litigants, surreptitious recording can hinder the work of law enforcement. Thereby, undermining the safety of the community as a whole. Regardless of whether this particular suggestion is adopted, informational safety must become a top priority for the judiciary, and protective measures must be adopted to reflect that.

---

27. *See* Stoney Brooks, *Does Personal Social Media Usage Affect Efficiency and Well-being?* 46 COMPUT. IN HUM. BEHAV. 26, 35 (2015) ("[S]ocial media usage is associated with lower task performance, increased technostress, and lower happiness."); *see also* Xiongfei Cao & Lingling Yu, *Exploring the Influence of Excessive Social Media Use at Work: A Three-Dimension Usage Perspective*, 46 INT'L J. OF INFO. MGMT. 83, 83 (2019) (explaining that the various types of social media use at work "decrease employee job performance" based on "[a]n empirical study of 305 social media users . . . "); Stoney Brooks & Christopher Califf, *Social Media-Induced Technostress: Its Impact on the Job Performance of IT Professionals and the Moderating Role of Job Characteristics*, 114 COMPUT. NETWORKS 143, 143 (2017) (discussing research that showed "that social media-induced technostress is negatively related to job performance . . . ").