SMU Science and Technology Law Review

Volume 24 | Number 2 Article 2

2021

The Communitarian Deficit in the USA: Three Telling Cases

Amitai Etzioni
The George Washington University

Author(s) ORCID Identifier:
https://orcid.org/0000-0002-2324-5890

THE COMMUNITARIAN DEFICIT IN THE USA: THREE TELLING CASES

*Amitai Etzioni**

ABSTRACT

Liberal communitarianism suggests that the balance between individual rights and the common good must be adjusted as historical conditions change.[1] Much attention has been paid to violations of rights, e.g., by the police, for good reasons. This Article examines three new technologies that undermine public safety, a key common good, and asks whether they should be banned.

The 2020 pandemic revealed that scores of millions of Americans objected, not merely to government mandates to take measures that are likely to spare fellow Americans a severe disease or death, but even to respond to moral calls, especially wearing a mask.[2] This Article examines three other areas which exhibit the same communitarian deficit.

The best-known version of communitarianism is the East Asian school, which puts great emphasis on the value of the common good and one's obligations to the community.[3] This school of thought tends to view the individual as a cell that is part of an organic whole and meaning is derived from contributions to whole. In this version of communitarianism, there is no fundamental place for liberty or individual rights, although some may be granted, if doing so helps the common good.[4]

---

* Amitai Etzioni, University Professor, Professor of international relations, and Director of the Institute for Communitarian Policy Studies at George Washington University. Former Author of Reclaiming Patriotism (University of Virginia Press, 2019), founder and curator of CivilDialogues.org. The author is indebted to Maari Weiss for extensive research assistance on this article.

1. Amitai Etzioni, *Communitarianism Revisited*, 19:3 J. POL. IDEOLOGIES 241, 241-60 (2014), https://www.uv.es/sasece/docum2015/Etzioni%20Communitarianism%20Revisited.pdf [https://perma.cc/65GU-E5X6].

2. *See* Jim Key, *Half of U.S. Adults Don't Wear Masks When in Close Contact with Non-Household Members*, USC DORNSIFE (Jan. 21, 2021), https://dornsife.usc.edu/news/stories/3388/understanding-coronavirus-in-america-mask-use-among-us-adults/ [https://perma.cc/BP6A-BTRR].

3. Amitai Etzioni, *Communitarianism – A Synthesis: Rights and Responsibilities*, ENCYLOPÆDIA BRITANNICA (Sept. 25, 2013), https://www.britannica.com/topic/communitarianism [https://perma.cc/CG3W-NC6F].

4. *See Late Singapore Leader Lee Kuan Yew Had Opinions on Everything*, TIME MAG. (Mar. 15, 2015), https://time.com/3748654/singapore-lee-kuan-yews-opinions/ [https://perma.cc/4F6Z-KD2Y]; WM. THEODORE DE BARY, ASIAN VALUES AND HUMAN RIGHTS: A CONFUCIAN COMMUNITARIAN PERSPECTIVE (Harvard Univ. Press 2000).

East Asian communitarianism is roundly rejected by Western intellectuals and all others who consider individual rights and liberty a core value.[5] Liberal communitarianism has corrected the main flaw of the Asian version by combining two fundamentally opposing philosophies: liberalism and communitarianism.[6] Liberal communitarianism assumes from the outset that a society ought to treat both individual rights and the common good as basic moral principles and that neither should be assumed to *a priori* trump the other.[7] It does not overlook the fundamentally incompatible nature of liberalism and communitarianism; rather, it seeks to embrace their incompatibilities, because one's strength is the other's deficiency.[8] Liberal communitarians recommend a constant balancing of the two sets of moral principles, requiring legislators and citizens alike to weigh the common good against individual rights to create policies and social norms that protect both.[9] When the common good and liberty come into conflict, liberal communitarians must rule which should take precedence.[10]

The Fourth Amendment captures extremely well the basic liberal communitarian thesis.[11] Unlike the First Amendment, which states that "Congress shall make no law,"[12] the Fourth protects against "unreasonable searches and seizures,"[13] which on the face of it recognizes a whole category of searches and seizures that are constitutional—those that are reasonable, i.e., in the public interest.[14] Moreover, the Fourth Amendment provides a mechanism for determining when searches and seizures are allowed: the courts.[15] The courts, in turn, are affected by and have an influence on the public discourse as well as the legislature.[16]

Societies constantly correct the balance between individual rights and social responsibilities as historical conditions change. Thus, after the 2001 attacks on the U.S. homeland, Congress rushed through a series of new se-

5. *See* Etzioni, *supra* note 3.

6. *Liberal Communitarianism: An Interview with Amitai Etzioni at 92*, 58 Soc'y 22, 22-25 (2021), https://link.springer.com/article/10.1007/s12115-021-00568-w [https://perma.cc/383T-XW9S].

7. *See* Etzioni, *supra* note 3.

8. *See id.*

9. *See id.*

10. *See id.*

11. U.S. CONST. amend. IV.

12. U.S. CONST. amend. I.

13. U.S. CONST. amend. IV.

14. *See id.*

15. *See id.*

16. *See id.*

curity measures.[17] When no new such attacks occurred over the next decade, these measures where reigned in. In short, liberal communitarians hold that no society can or should be designed according to one set of principles, that they can be more liberal or more communitarian, and that the relative weight accorded to the two sets of principles much change within history.[18]

Recently, much attention has been paid in the United States, for very compelling reasons, to violations of individual rights by the police, to racism embedded in many American institutions, and to high tech corporations that invade privacy among others.[19] A cursory examination of the daily press will find many more such reports. More attention should be paid to those instances in which the imbalance is titled the other way: the common good is unduly neglected. Three case studies follow, each of considerable weight in terms of the scope of their effects on public safety, arguably the leading common good, or what the courts tend call the public interest.

I. POWERFUL ENCRYPTION

For many decades, law enforcement authorities in the United States have been able to obtain warrants or court orders to monitor criminals (including drug dealers, human traffickers, and terrorists) by listening to phone conversations and reading cables, faxes, and—more recently—emails and text messages, all without undue difficulties.[20] Since 1994, much of this work has been facilitated by the Communications Assistance for Law Enforcement Act (CALEA), a law "requiring telecommunications companies to build into their systems an ability to carry out a wiretap order if presented with one."[21] (The CIA and the NSA similarly conduct surveillance using communication technology, the former primarily overseas and the latter both overseas and domestically). Frequently, law enforcement and security agencies (collectively, public authorities) could carry out their surveillance without the

17. Jason Villemez, *9/11 to Now: Ways We Have Changed*, PBS NEWS HOUR (Sept. 14, 2011), https://www.pbs.org/newshour/world/911-to-now-ways-we-have-changed [https://perma.cc/CVG9-US94].

18. *See* Etzioni, *supra* note 1.

19. Brian X. Chen, *When You Should (and Shouldn't) Share Your Location Using a Smartphone*, N.Y. TIMES (July 12, 2017), https://www.nytimes.com/2017/07/12/technology/personaltech/using-location-sharing-apps.html [https://perma.cc/KGB4-C6CX].

20. *See* Theodoric Meyer, *No Warrant, No Problem: How the Government Can Get Your Digital Data*, PROPUBLICA (Jun. 27, 2014), https://www.propublica.org/article/no-warrant-no-problem-how-the-government-can-still-get-your-digital-data [https://perma.cc/42BM-ZPTG].

21. David E. Sanger & Brian X. Chen, *Signaling Post-Snowden Era, New iPhone Locks Out N.S.A.*, N.Y. TIMES (Sept. 26, 2014), https://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html [https://perma.cc/9SP6-4C7Z].

knowledge of the parties under observation.[22] However, unlike telecommunications companies, technology companies are not bound by CALEA, and the law therefore does not guarantee public authorities' access to emails or to data contained on a smartphone.[23] And then came the very strong end-to-end encryption.

Over the centuries, indeed millennia, there has been a sort of arms race between those trying to protect the privacy of their messages, using various techniques, and those trying to decipher them.[24] The most recent privacy protection measure, end-to-end encryption, is particularly powerful.[25] With end-to-end encryption, a message is only readable on the devices of the sender and the intended recipient; messages sent with end-to-end encryption that are intercepted cannot be "read."[26] Outside of the sender and recipient, anyone trying to gain access to the messages, whether legally or illegally, "must hack directly into the sender's or recipient's device, something that can be harder to do 'at scale' and makes mass surveillance much more difficult."[27] The question this development raises; Does this software/technological development tip the scale too far against public safety, considering the need to fight crime, avoid domestic terrorism, and identify international threats?

Two intersecting questions are at issue in the debate over end-to-end encryption. First, should any private corporation be allowed to market a tool that severely stymies the work of public authorities? One can seek to answer this question abstractly, in which case I would argue for allowing private parties to provide people with a high level of protection, sufficient to guard against intrusion from most other private parties (ex-spouses, competitors, media, etc.) and most hackers, but not from public authorities that have obtained a warrant or court order and have stronger surveillance technologies. The Fourth Amendment to the Constitution protects people "against *unreasonable* searches and seizures."[28] That is, it allows for searches that are in the public interest. Courts rule what is reasonable. However, end-to-end encryption prevents the execution of reasonable searches.

Most importantly, one should address this question within history, in line with the liberal communitarian principle that holds that historical context

22. *See* Meyer, *supra* note 20.

23. Matt Apuzzo, David E. Sanger & Michael S. Schmidt, *Apple and Other Tech Companies Tangle With U.S. Over Data Access*, N.Y. TIMES (Sept. 7, 2015), https://www.nytimes.com/2015/09/08/us/politics/apple-and-other-tech-companies-tangle-with-us-over-access-to-data.html [https://perma.cc/JJF8-S64Q].

24. *See* Nicole Perlroth, *What Is End-to-End Encryption? Another Bull's-Eye on Big Tech*, N.Y. TIMES (Nov. 19, 2019), https://www.nytimes.com/2019/11/19/technology/end-to-end-encryption.html [https://perma.cc/HR7Y-3FNP].

25. *See id.*

26. *Id.*

27. *Id.*

28. U.S. CONST. amend. IV.

may influence and lead to adjustments in the balance between individual rights and the common good, in this case public safety. What is the current condition in the United States?

A. The State of Public Safety in the United States

In the United States in 2019, 38.6 percent of murder cases, about half (47.7 percent) of aggravated assault offenses, and more than eight out of ten (82.8 percent) of all property crimes were not cleared by law enforcement.[29] The government is unable to stem the flood of controlled substances from other nations, contributing to the overdose deaths of over 90,000 people in the United States in 2020 alone.[30] Human trafficking and illegal currency also continue to flow at high levels.[31] There is a considerable increase of domestic terrorism and hate crimes.[32] In March 2021, Alejandro Mayorkas, the Secretary of the Department of Homeland Security, testified before the House Homeland Security Committee, stating, "While we remain vigilant about the threat of foreign terrorism, ideologically motivated domestic violent extremism now poses the most lethal and persistent terrorism-related threat to the homeland today."[33] Public safety is much higher in other liberal democracies.

Additional complications arise when dealing with terrorism cases that have foreign connections. For example, when then-Federal Bureau of Investigation (FBI) director James B. Comey testified before a Senate committee in December 2015, he discussed the ways encryption was hampering the investigation into a shooting in Garland, Texas for which the Islamic State had

29. FED. BUREAU OF INVESTIGATION, UNIF. CRIME REPORTING, 2019 CRIME IN THE U.S.: CLEARANCES (2019), https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019/topic-pages/clearances [https://perma.cc/K9BZ-KU8Z].

30. Brian Mann, *U.S.-Mexico Efforts Targeting Drug Cartels Have Unraveled, Top DEA Official Says*, NPR (May 3, 2021), https://www.npr.org/2021/05/03/993059731/u-s-mexico-efforts-targeting-drug-cartels-have-unraveled-top-dea-official-tells- [https://perma.cc/38MV-J5L6].

31. *See* FED. BUREAU OF INVESTIGATION, UNIF. CRIME REPORTING, 2019 CRIME IN THE U.S.: HUMAN TRAFFICKING (2019), https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019/additional-data-collections/human-trafficking [https://perma.cc/CXE9-U3ZS]; William J. Luther, *How Much Cash is Used by Criminals and Tax Cheats?*, AM. INST. FOR ECON. RSCH. (Feb. 8, 2017), https://www.aier.org/article/how-much-cash-is-used-by-criminals-and-tax-cheats/ [https://perma.cc/65HT-U4YD].

32. *See* Ellen Nakashima, *Domestic Terrorism Poses 'Elevated Threat' to the U.S. This Year, Intelligence Agencies Say in Their First Joint Report on the Issue*, WASH. POST (Mar. 17, 2021, 6:55 PM), https://www.washingtonpost.com/national-security/domestic-extremism-threat-intelligence-community-assessment/2021/03/17/05c9e712-8759-11eb-bfdf-4d36dab83a6d_story.html [https://perma.cc/2KJH-AUJV].

33. *Id.*

claimed responsibility.[34] Comey "told the Senate Judiciary that one of the attackers 'exchanged 109 messages with an overseas terrorist' the morning of the shooting," and the messages were unreadable due to encryption.[35]

In short, U.S. public safety is not well protected. In the U.S., private corporations are free to invest in whatever technologies they wish and market them aggressively, whatever the public outcome.[36] The public is usually forced to adapt. In rare conditions, when the social costs are very high, some post hoc attempts are made to curb the effects. Should end-to-end encryption be one of those rare exceptions?

B. Living with End-to-End Encryption

In the following examination of the issue at hand, this Article focuses on one corporation, Apple, not merely because it aggressively marketed end-to-end encryption, but also because it added another feature to protect the privacy of the messages—a particular password.[37] Ten incorrect attempts to overcome the password in a row leads to the erasure of data stored on an Apple iPhone.[38] This feature prevents law enforcement from using computers to break the password and read the messages—even if they happen to have the phone of the criminal or terrorist.[39] Finally, Apple has frequently taken the lead in relevant court cases—to protect privacy protection technologies.[40]

---

34. David E. Sanger & Nicole Perlroth, *F.B.I. Chief Says Texas Gunman Used Encryption to Text Overseas Terrorist*, N.Y. Times (Dec. 10, 2015), https://www.nytimes.com/2015/12/10/us/politics/fbi-chief-says-texas-gunman-used-encryption-to-text-overseas-terrorist.html [https://perma.cc/P47T-MUH7].

35. *Id.*

36. *See* Vikramaditya Khanna, *Holding Corporations and Executives Accountable Depends on Our Legal System*, ProMarket (Mar. 14, 2021), https://promarket.org/2021/03/14/corporations-executives-accountability-wrongdoing-legal-system/ [https://perma.cc/Q7LT-44L6].

37. Avery Hartmans, *There's a Scary iPhone Feature that Erases All your Data After Too Many Password Attempts – Here's Why you Should Turn it on Anyway*, Bus. Insider (Dec. 16, 2018, 2:10 PM), https://www.businessinsider.com/iphone-security-failed-passcode-attempts-2018-6 [https://perma.cc/9T5C-Q9ZZ].

38. *Id.*

39. See Ellen Nakashima, *Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks*, Wash. Post (Feb. 17, 2016), https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html [https://perma.cc/DN3N-VLX6].

40. *See* Arjun Kharpal, *Apple vs FBI: All You Need to Know*, CNBC (Mar. 29, 2016), https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html [https://perma.cc/U83X-7V47].

The fact is that end-to-end encryption is out there and cannot be rolled back any more than the proverbial genie can be enticed back into the bottle. This leads to the second question in the debate over end-to-end encryption: What can be done now that end-to-end encryption exists and has become common? It is a limited question, akin to asking if, after the house burned down, who will own the ashes? We are dealing with those relatively rare cases in which the authorities do have the phone of a criminal, and a warrant or court order to search it, should they be able to overcome the phone passcode in order to access the data stored on the phone? Note that this limited form of damage control, leaving not just criminals but also authoritarian regimes free to use end-to-end encryption with impunity most of the time.

After the December 2015 terrorist attack in San Bernardino, California, a dispute arose between the FBI and Apple regarding access to the data on an iPhone used by one of the terrorists.[41] Apple refused to help the FBI circumvent the iPhone's password in order to gain the information contained in the locked phone.[42] The FBI took the case to court, arguing that it needed Apple's help to retrieve information that could prove pertinent to the investigation of the terrorist attack.[43] Apple continued to object, even after a court issued an order, i.e., defined the FBI's request as constitutional.[44] The particular case became moot when a third party, paid by the FBI, was able to open into the phone.[45]

The issue, however, stands: Should private companies be allowed to provide the public with end-to-end encryption and related passwords that makes it extremely difficult for public authorities to discharge their duties?[46] Are privacy and other human rights advocates correct that if end-to-end encryption had a "backdoor," an opening that could be exploited to by public authorities, rights would be endangered?[47] Is there a way to protect individual rights and still enable public authorities to carry out their duties?

C. Individual Rights Perspective

Individual rights advocates "argue that end-to-end encryption steers governments away from mass surveillance and toward a more targeted, constitutional form of intelligence gathering."[48] Because governments cannot easily vacuum up data sent with end-to-end encryption, this form of encryption serves to protect the privacy, free expression, and activism of individuals

41. *Id.*
42. *Id.*
43. *Id.*
44. Nakashima, *supra* note 39.
45. Kharpal, *supra* note 40.
46. *See* Perlroth, *supra* note 24.
47. *See id.*
48. *Id.*

and communities around the world. However, one notes, this form of encryption stymies all surveillance, including surveillance that is constitutional.

Apple chief executive Tim Cook's public "Customer Letter," released during the San Bernardino dispute, warned of a slippery slope if the government prevailed in court:

> The government suggests this tool could only be used once, on one phone. But that's simply not true. Once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks—from restaurants and banks to stores and homes. No reasonable person would find that acceptable.[49]

He elaborated:

> The implications of the government's demands are chilling. If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge.[50]

The *New York Times* reports that "[p]rivacy activists and security experts noted that any back door created for United States law enforcement agencies would inevitably become a target for foreign adversaries, cybercriminals and terrorists."[51] A former chief security officer at Yahoo and current Stanford professor, Alex Stamos, stated that intentionally making a backdoor to encryption is akin to "drilling a hole in the windshield."[52] In his "Customer Letter," Cook argued that forcing Apple to create a backdoor "would hurt only the well-meaning and law-abiding citizens who rely on companies like Apple to protect their data.[53] Criminals and bad actors will still encrypt, using tools that are readily available to them."[54]

---

49. Tim Cook, *Customer Letter*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/ [https://perma.cc/237L-SGFJ].

50. *Id.*

51. Perlroth, *supra* note 24.

52. *Id.*

53. Cook, *supra* note 49.

54. *Id.*

D. Public Safety Perspective

One of the most prominent arguments against the use of end-to-end encryption without backdoors is the claim that such encryption impedes law enforcement investigations, thereby putting public safety at risk. Public authorities report "that end-to-end encryption makes it much harder to track terrorists, pedophiles and human traffickers."[55] In a 2014 speech, then-FBI director Comey stated that the FBI refers to the public safety issues created by these technologies as "Going Dark," and what it means is this:

> Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so.[56]

Later in his speech, Comey stated, "Sophisticated criminals will come to count on these means of evading detection. It's the equivalent of a closet that can't be opened. A safe that can't be cracked."[57] In 2018, a Baton Rouge district attorney held that Apple is "blatantly protecting criminal activity, and only under the guise of privacy for their clients."[58]

With end-to-end encryption, public authorities cannot surveil the messages of people believed to be engaging in criminal activity, even when they have a legal warrant or court order to do so.[59] Furthermore, when the government has possession of a phone (or other encrypted communication devices and places data are stored) of proven criminals, investigators generally need expensive tools (or the help of corporations that specialize in legal hacking) in order to gain access.[60]

These are time-consuming undertakings: "a six-digit iPhone passcode takes on average about 11 hours to guess, while a 10-digit code takes 12.5

---

55. Perlroth, *supra* note 24.

56. James B. Comey, *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?*, Fed. Bureau Investigation (Oct. 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course [https://perma.cc/866H-LQYA].

57. *Id.*

58. Jack Nicas, *Apple to Close iPhone Security Hole That Law Enforcement Uses to Crack Devices*, N.Y. Times (June 13, 2018), https://www.nytimes.com/2018/06/13/technology/apple-iphone-police.html [https://perma.cc/8YUY-ZDZ6].

59. *See* Susan Landau, *Law Enforcement Is Accessing Locked Devices Quite Well, Thank You*, Lawfare (Dec. 7, 2020), https://www.lawfareblog.com/law-enforcement-accessing-locked-devices-quite-well-thank-you [https://perma.cc/62JE-RUP7].

60. *See id.*

years."[61] In 2019, Manhattan district attorney Cyrus R. Vance Jr. testified before Congress, stating, "We may unlock it in a week, we may not unlock it for two years, or we may never unlock it."[62] Thus, while the phone may eventually be forced open and yield its information, this approach often does not solve the problem that law enforcement agencies face, because investigations are often urgent and time-sensitive.[63] As Vance put it, "Murder, rape, robberies, sexual assault. I do not mean to be dramatic, but there are many, many serious cases where we can't access the device in the time period where it is most important for us."[64] Of special concern are the many situations in which rapid action is required, as when criminal activities are ongoing.

E. A Third Way

Both sides in this debate have staked out extreme views. In 2018, the *Washington Post* reported that "[t]he FBI ha[d] repeatedly provided grossly inflated statistics to Congress and the public about the extent of problems posed by encrypted cellphones."[65] On the other hand, Apple, cybersecurity experts, and privacy activists tend to present encryption as a largely all-or-nothing form of protection, in which consumer data is either completely secure or completely vulnerable.[66]

A leading concern is that democratic governments' unauthorized use of data will enable authoritarian governments to continue breaching citizen's privacy and help them impose their rule. Essentially, data security protections would degrade globally if the U.S. were to allow greater data access by government authorities. Senator Ron Wyden stated, "This move by the FBI could snowball around the world. Why in the world would our government want to give repressive regimes in Russia and China a blueprint for forcing American companies to create a backdoor?"[67] Authoritarian governments

61. Jack Nicas, *The Police Can Probably Break Into Your Phone*, N.Y. TIMES (Oct. 21, 2020), https://www.nytimes.com/2020/10/21/technology/iphone-encryption-police.html [https://perma.cc/8GUG-K].

62. *Id.*

63. *See id.*

64. *Id.*

65. Devlin Barrett, *FBI Repeatedly Overstated Encryption Threat Figures to Congress, Public*, WASH. POST (May 22, 2018), https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html [https://perma.cc/DYN9-EP9A].

66. *See* Cook, *supra* note 49; *Australia Data Encryption Laws Explained*, BBC NEWS (Dec. 7, 2018), https://www.bbc.com/news/world-australia-46463029 [https://perma.cc/RA57-3MGF].

67. Spencer Ackerman, *Apple Encryption Case Risks Influencing Russia and China, Privacy Experts Say*, GUARDIAN (Feb. 17, 2016), https://

these days have plenty of tools and are quite able to develop more if they feel they need them, as China did with facial recognition.[68] However, if democratic governments are unable to maintain a reasonable level of public safety, it will undermine their legitimacy and sustainability.

As to the argument that the ability to gain covert access to digital data will lead to the U.S. government surveilling too much or inappropriately, this should be dealt with by tightening congressional and local oversight of federal and local public authorities and by increasing accountability, not by preventing access or making it so burdensome as to delay investigations that need to be carried as crimes occur or are in short pursuit.

Most importantly, the choice is not between making the phones and their data vulnerable to hacking by anyone who pays for some software online or buys a device from RadioShack, or locking them so tightly that it is extremely difficult even for the FBI to decrypt them—especially in many situations in which time is of the essence, such as during a terrorist attack or kidnapping. Instead, Apple and other such corporations, should, if a court rules that the FBI (or another public authority) has a right to investigate a case, at least grant access to the particular phone involved.

This is what happened until September 2014. Up to that point, Vance, the Manhattan district attorney, would get warrants or court orders and send phones to Apple, which did open them and send the information to Vance, without giving him a key.[69] Apple stopped participating in this process after it began encrypting its phones by default and ended its practice of keeping a digital key that could unlock its devices.[70] The company publicized its decision to take these steps, and some hold that the move was part of Apple's new marketing strategy.[71]

In a telling development—which speaks volumes about Silicon Valley's libertarian culture—Apple turned to the courts in 2021 to try to gain informa-

www.theguardian.com/technology/2016/feb/17/apple-fbi-encryption-san-bernardino-russia-china [https://perma.cc/U9P4-Q4UK].

68. *See* Eva Dou, *China Built the World's Largest Facial Recognition System. Now, it's Getting Camera-Shy*, WASH. POST (July 30, 2021), https://www.washingtonpost.com/world/facial-recognition-china-tech-data/2021/07/30/404c2e96-f049-11eb-81b2-9b7061a582d8_story.html [https://perma.cc/LY5M-DVW6].

69. Cyrus R. Vance, Jr., N.Y. Dist. Att'y, *Privacy and Security in the Digital Age*, COUNCIL ON FOREIGN RELS. (May 11, 2016), https://www.cfr.org/event/privacy-and-security-digital-age [https://perma.cc/NBN6-NLQN].

70. L. Gordon Crovitz, Partner at NextNews Ventures, *Privacy and Security in the Digital Age*, COUNCIL ON FOREIGN RELS. (May 11, 2016), https://www.cfr.org/event/privacy-and-security-digital-age [https://perma.cc/NBN6-NLQN].

71. *See* Adam Segal, Dir., Digit. and Cyberspace Pol'y Program, Council on Foreign Rels., *Privacy and Security in the Digital Age*, COUNCIL ON FOREIGN RELS. (May 11, 2016), https://www.cfr.org/event/privacy-and-security-digital-age [https://perma.cc/NBN6-NLQN].

tion about the ways the FBI has been able to read their phones in order to enable Apple to close the weakness, which would prevent the FBI from discharging its court-approved duties in the future.[72]

Apple's commitment to protect the privacy of its customers melted like the early spring fog when it needed to protect its very lucrative business in China.[73] Nearly every Apple product is assembled in China, and the Chinese provide twenty percent of the company's revenue.[74] The Chinese government and Apple have forged an agreement that effectively skirts U.S. law banning U.S. companies from providing Chinese law enforcement with data.[75] According to the agreement, Apple customers' data are owned not by Apple but by Guizhou-Cloud Big Data (GCBD), which is owned by the Guizhou Province government.[76] Further, in accordance with a law mandating China-based storage for personal and important data gathered in China, Apple is opening a data center in the capital of Guizhou Province that will store Chinese customers' personal data.[77] A *New York Times* investigation found that, "in its data centers, Apple's compromises have made it nearly impossible for the company to stop the Chinese government from gaining access to the emails, photos, documents, contacts and locations of millions of Chinese residents . . ."[78] Specifically, the *New York Times* reports: "Chinese state employees physically manage the computers. Apple abandoned the encryption technology it used elsewhere after China would not allow it. And the digital keys that unlock information on those computers are stored in the data centers they're meant to secure."[79]

For the rest of the world the issue stands: Should a private company be allowed, by law, to block public authorities, even when the courts have ruled that their search is a legal one? More generally, should private corporations be able to spring upon society whatever technology they seek to develop and market? Deepfake videos and communications? Artificial Intelligence (AI) for automatic weapons that cannot be recalled once launched? A liberal com-

72. Ellen Nakashima & Reed Albergotti, *The FBI Wanted to Unlock the San Bernardino Shooter's iPhone. It Turned to a Little-Known Australian Firm*, WASH. POST (Apr. 14, 2021, 8:00 AM), https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/ [https://perma.cc/L2X6-Y942].

73. *See* Jack Nicas, Raymond Zhong, & Daisuke Wakabayashi, *Censorship, Surveillance and Profits: A Hard Bargain for Apple in China*, N.Y. TIMES (May 17, 2021), https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html [https://perma.cc/VV6T-UDFW].

74. *Id.*

75. *See id.*

76. *Id.*

77. *See id.*

78. *Id.*

79. Nicas, *supra* note 73.

munitarian answer is that there is a need to enhance the capacity of society to review new technologies and when they cause great social harm, to curb their use.

Much depends on the specific technology and the historical conditions. Given the poor state of public safety in the United States, ideally end-to-end encryption should never have been introduced. But because end-to-end encryption cannot be removed, public authorities should at least have timely access to the phones of criminals, in the rare cases they have access to them, once the courts so ordered. This can be achieved by collaboration of the technology corporations involved, without weakening the privacy of all the other users.

II. CRYPTOCURRENCY: SHOULD BE BANNED

Cryptocurrencies are a significant factor in the global financial system. The combined value of existing cryptocurrencies reached $2.4 trillion in 2021, double that of the U.S. dollar.[80] This section of the Article focuses on Bitcoin, because it was the first cryptocurrency, and its existence paved the way for this new financial factor.[81]

The term "Bitcoin" refers to both the currency itself and the payment network in which the currency exists.[82] "Bitcoin is a digital token—with no physical backing—that can be sent electronically from one user to another, anywhere in the world."[83] Bitcoins can be divided into much smaller amounts than traditional currencies; the smallest unit in the Bitcoin system is 0.00000001 Bitcoins.[84] Once 21 million Bitcoins exist, a milestone that, as of 2017, was estimated to be over 120 years away, the total supply of Bitcoins is capped, as it is not possible to introduce any more Bitcoins into the global marketplace.[85] The Bitcoin payment network is a "system [that] is run by a decentralized network of computers around the world that keep track of all Bitcoin interactions, similar to the way Wikipedia is maintained by a decentralized network of writers and editors."[86]

80. Eric Lipton, *As Scrutiny of Cryptocurrency Grows, the Industry Turns to K Street*, N.Y. TIMES (May 9, 2021), https://www.nytimes.com/2021/05/09/us/politics/cryptocurrency-regulation-sec-ripple-labs.html [https://perma.cc/J3LK-RNFF].

81. *Id.*

82. Nathaniel Popper, *What Is Bitcoin, and How Does It Work?,* N.Y. TIMES (Oct. 1, 2017), https://www.nytimes.com/2017/10/01/technology/what-is-bitcoin-price.html [https://perma.cc/289F-CEMG].

83. *Id.*

84. *Id.*

85. *Id.*

86. *Id.*

A. Bitcoin and Crime

People seeking to engage in illegal or covert activity, from criminals to foreign adversaries, have found that Bitcoin is conducive to their efforts.[87] "Criminals have taken to Bitcoin because anyone can open a Bitcoin address and start sending and receiving Bitcoins without giving a name or identity. There is no central authority that could collect this information."[88] The lack of a central authority is one of the features that distinguishes Bitcoin from traditional exchange systems; PayPal, for example, is a company that can function as a gatekeeper and that has the power to freeze and shut down accounts, while Bitcoin does not have these capabilities.[89]

The U.S. government has successfully sanctioned specific digital Bitcoin wallets, demonstrating that "the United States Treasury can disrupt cryptocurrency trades, even if only a miniscule fraction of the total."[90] However, such relief is not permanent, or even long-lasting. "New anonymous wallets can be created for free within minutes."[91] For instance, due to the difficulty associated with tracing Bitcoin transactions, Iranians, as well as businesses that are interested in doing business with Iranians, have found the currency to be useful in circumventing U.S. banking sanctions against Iran.[92] Furthermore, Bitcoin does not have to abide by the law that requires banks to report transactions of $10,000 or more.[93]

Drug markets on the dark web are often reliant on Bitcoin. Synthetic opioids such as fentanyl can be made in China, exchanged for Bitcoin on the dark web, and shipped to users around the world, a practice that has contrib-

87. *See* Nathaniel Popper, *Dark Web Drug Sellers Dodge Police Crackdowns*, N.Y. Times (June 11, 2019), https://www.nytimes.com/2019/06/11/technology/online-dark-web-drug-markets.html [https://perma.cc/TE5X-7PTA]; Nathaniel Popper & Matthew Rosenberg, *How Russian Spies Hid Behind Bitcoin in Hacking Campaign*, N.Y. Times (July 13, 2018), https://www.nytimes.com/2018/07/13/technology/bitcoin-russian-hacking.html [https://perma.cc/PE4Y-7PZW].

88. Popper, *supra* note 82.

89. Nathaniel Popper, *Terrorists Turn to Bitcoin for Funding, and They're Learning Fast*, N.Y. Times (Aug. 18, 2019), https://www.nytimes.com/2019/08/18/technology/terrorists-bitcoin.html [https://perma.cc/EBT6-MRYP].

90. Thomas Erdbrink, *How Bitcoin Could Help Iran Undermine U.S. Sanctions*, N.Y. Times (Jan. 29, 2019), https://www.nytimes.com/2019/01/29/world/middleeast/bitcoin-iran-sanctions.html [https://perma.cc/3LD4-667Z].

91. *Id.*

92. *Id.*

93. *See* MacKenzie Sigalos, *How the IRS is Trying to Nail Crypto Tax Dodgers*, CNBC (July 14, 2021, 12:08 PM), https://www.cnbc.com/2021/07/14/irs-new-rules-on-bitcoin-ethereum-dogecoin-trading.html [https://perma.cc/7CBB-KZBR].

uted to the U.S. opioid epidemic.[94] Although the authorities have been able to take down some of the popular dark web sites, there are always other sites available. For example, after the authorities shut down the Silk Road, an infamous site on the dark web, in 2013, drug dealers moved to other sites.[95] And, "in 2017, when the police took down two of the biggest successors to Silk Road, AlphaBay and Hansa market, there was five times as much traffic on the dark net as the Silk Road had at its peak."[96] As of 2019, online drug markets using Bitcoin were responsible for annual commerce amounting to almost $1 billion.[97]

Criminals operating in other channels have also gravitated towards Bitcoin.[98] The Russian operatives that interfered with the 2016 presidential election as well as those who targeted Hillary Clinton's campaign, relied extensively on Bitcoin to finance much of the technological infrastructure of their hacking endeavors.[99] "Bitcoin has also become the standard currency for ransomware operations in which victims lose control of their computer to remote hackers. Victims are able to get back their files only if they send a Bitcoin payment."[100] These attacks have a wide range of targets, from individuals to hospitals and government agencies.[101] In 2021, the operator of a critical fuel pipeline on the East Coast paid extortionists in Bitcoin to recover its data.[102] As senior threat intelligence analyst Curt Wilson put it, "The criminal underground very much likes Bitcoin. It's enabled a greater sense of obfuscation."[103] Further, for victims, Bitcoin payments add to the pain of the

94. Caitilin Reilly, *Cryptocurrencies Complicate Effort to Stop Opioid Dealers*, ROLL CALL (Oct. 29, 2019, 6:31 AM), https://www.rollcall.com/2019/10/29/cryptocurrencies-complicate-effort-to-stop-opioid-dealers/ [https://perma.cc/3DX4-VZV9].

95. Popper, *supra* note 87.

96. *Id.*

97. Popper, *supra* note 89.

98. *See* Popper & Rosenberg, *supra* note 87.

99. *Id.*

100. Alan Rappeport & Nathaniel Popper, *Cryptocurrencies Pose National Security Threat, Mnuchin Says*, N.Y. TIMES (July 15, 2019), https://www.nytimes.com/2019/07/15/us/politics/mnuchin-facebook-libra-risk.html [https://perma.cc/ZT5W-UPDL].

101. Erdbrink, *supra* note 90; Nathaniel Popper, *For Ransom, Bitcoin Replaces the Bag of Bills*, N.Y. TIMES (July 25, 2015), https://www.nytimes.com/2015/07/26/business/dealbook/for-ransom-bitcoin-replaces-the-bag-of-bills.html [https://perma.cc/9RHY-KSUA].

102. Michael D. Shear, Nicole Perlroth & Clifford Krauss, *Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers*, N.Y. TIMES (May 14, 2021), https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html [https://perma.cc/3GKA-J3QU].

103. Popper, *supra* note 87.

attack, because, unlike transactions carried out through PayPal or credit card companies, there is no way to recoup losses incurred through Bitcoin.[104]

In April 2021, the commissioner of the Internal Revenue Service, Charles Rettig, estimated that unpaid taxes, primarily stemming from tax evasion by large corporations and wealthy individuals, account for about $1 trillion in lost annual revenue.[105] Rettig laid some of the blame for the growth in this "tax gap" on cryptocurrency and the light regulation that surrounds that sector of the financial markets.[106]

In recent years, terrorist organizations, which are often unable to utilize the traditional financial system, have discovered the benefits of Bitcoin, and they have begun to use the currency in their fundraising endeavors.[107] For example, the Al Qassam Brigades, the military wing of Hamas, created a website in which "every visitor is given a unique Bitcoin address where he or she can send the digital currency, a method that makes the donations nearly impossible for law enforcement to track."[108] A video on the site provides instructions and teaches potential donors how to avoid attracting the attention of the authorities as they go through the necessary steps to obtain Bitcoin and transmit it to the terrorists.[109] The chief executive of an Israeli intelligence company that monitors the block chain, Itsik Levy, stated: "The terrorists are learning how to send and receive digital currency in a smarter way. Why would terrorists not take advantage of this? It is great for them."[110] Even relatively small sums raised through fundraising campaigns that rely on Bitcoin can have a significant impact, as little payments are proving increasingly difficult to track and terrorist attacks are not expensive.[111]

B. Bitcoin's Defenders

Bitcoin's champions refer to several reasons to explain their support for the currency and exchange system. *NPR* provides a succinct summary:

> The cryptocurrency is free of politics, significant at a time when so many people mistrust the competence and intentions of government. It's not controlled by central banks or leaders craving popular approval. Bitcoin is borderless. Bitcoin can't be counterfeited,

104. *Id.*

105. Alan Rappeport, *Tax Cheats Cost the U.S. $1 Trillion per Year, IRS Chief Says*, N.Y. Times (Apr. 13, 2021), https://www.nytimes.com/2021/04/13/business/irs-tax-gap.html [https://perma.cc/6D3Q-Z9G6].

106. *Id.*

107. Popper, *supra* note 87.

108. *Id.*

109. *Id.*

110. *Id.*

111. *Id.*

> spent twice. And here's what might be the biggest argument of all on behalf of Bitcoin: The way it's designed, only 21 million Bitcoins will ever exist. So, like gold, it is finite, which makes it a hedge against inflation. In contrast, the maximalist argument goes, governments can print endless amounts of money. So, scarcity will keep Bitcoin valuable. There's only so much of it.[112]

However, several other cryptocurrencies are now available; criminals have access to all the dark currency they need.

C. Partial Treatments

There have been some attempts to reach a balance between the need to protect people from crime and the freedom and libertarian sensibilities associated with the use of cryptocurrencies. To combat the use of Bitcoin in ransomware attacks, some advocates have suggested that one could "digitally mark any coins used for ransom payments, similar to how dollar bills used in hostage situations are marked with invisible dye."[113] However, others are reluctant to accept this proposal, because they feel that it involves taking steps that would compromise the restriction-free nature of cryptocurrency transactions.[114] Lee Reiners, the executive director of Duke Law's Global Financial Markets Center, argues that cryptocurrencies are too convenient and valuable to criminals, especially ransomware attackers, to be allowed to proliferate.[115] He advocates in favor of banning—or, at the very least, seriously regulating—the use of all cryptocurrencies.[116]

> Cryptocurrency firms serving U.S. customers are supposed to be subject to the same anti-money-laundering requirements as traditional financial institutions, but more can be done. Late last year, the Treasury Department's Financial Crimes Enforcement Network proposed a rule to establish new reporting, verification and record-keeping requirements for certain cryptocurrency transactions. Last week, Treasury proposed granting more resources to the Internal Revenue Service to address crypto and called on businesses to report receipts of more than $10,000 in cryptocurrency.

112. Uri Berliner, *Bitcoin: Mother of All Bubbles, or Revolutionary Breakthrough*, NPR (Mar. 2, 2021), https://www.npr.org/2021/03/02/971745290/bitcoin-revolutionary-breakthrough-or-mother-of-all-bubbles [https://perma.cc/M332-9XUS].

113. Popper, *supra* note 87.

114. *Id.*

115. Lee Reiners, *Ban Cryptocurrency to Fight Ransomware*, WALL ST. J. (May 25, 2021), https://www.wsj.com/articles/ban-cryptocurrency-to-fight-ransomware-11621962831 [https://perma.cc/H862-WB3B].

116. *Id.*

> Both proposals should be adopted, but they will be effective only if other countries follow suit.[117]

One Wall Street observer put it clearly:

> Cryptocurrencies are for speculators, criminals, and cosplayers. Aside from that, they're useless, and I'm tired of everyone trying to pretend otherwise. I have waited for years for someone to explain to me a decent use case for cryptocurrencies. But throughout the recent fervor over crypto with its huge price boom and subsequent bust, I've yet to hear one . . . On the run from the US government because you helped plan the attack on the Capitol on January 6? Ask your followers to send crypto. Want to hack into the Colonial Pipeline and hold the company for a $5 million ransom without getting caught? Make your victims send you crypto.[118]

This seems a reasonable conclusion given the wide ranging and serious benefits the new currency provides to criminals, the inability of public authorities to track transactions in these currencies, even when there is incontestable evidence that they are used to violate the law. Unlike end-to-end encryption, which seems too entrenched to ban, even if the public and elected officials were included to ban it. Cryptocurrency, until very recently, was not accepted by respectable actors. It is a technology that one still might be able to ban, given the special profile it has: great harms to the common good and very few contributions to individual rights not readily available elsewhere.

III. FACIAL RECOGNITION: FIX NOT BAN

Facial recognition is a technological way of identifying an individual or confirming an individual's identity using their face. *Facial recognition* is used to identify people in photos, videos, or in real-time.[119] Panoramic, a private company, first began developing facial recognition technology in the 1960s, with funding that appears to have been provided by the Central Intelligence Agency and its front companies.[120] These early efforts faced signifi-

117. *Id.*

118. Linette Lopez, *Cryptocurrencies are for Speculators, Criminals, and Cosplayers. Other Than That, They're Useless*, BUS. INSIDER (May 26, 2021), https://www.businessinsider.com/crypto currencies-bitcoin-blockchain-useless-except-speculators-criminals-cosplayers-2021-5 [https://perma.cc/R3JK-ZEVH].

119. Shaun Raviv, *The Secret History of Facial Recognition*, WIRED (Jan 21, 2020, 6:00 AM), https://www.wired.com/story/secret-history-facial-recognition/ [https://perma.cc/DZW7-BUNL].

120. *Id.*

cant technological obstacles.[121] During the next three decades, others devised new methods by which technology could begin to recognize and differentiate faces. Public awareness of facial recognition rose in 2001, when law enforcement employed the technology to monitor Super Bowl crowds and police utilization of facial recognition tools became widespread.[122] It took off as computer power increased in the 2010s[123] and is now used regularly by public authorities in democratic societies and by authoritarian regimes, especially China.

A. Arguments in Favor of Government Use of Facial Recognition

The arguments in favor of government, particularly law enforcement, uses of facial recognition are fairly straightforward, centering around the technology's value as an investigatory and crime-solving tool. For example, in 2017, after investigators in Florida uncovered the identity of a suspect in an armed robbery.[124] Using facial recognition, they were able to find his girlfriend and share the surveillance footage with her.[125] She agreed that her boyfriend was the person in the video, which helped get him to plead guilty.[126] Similarly, in 2019, Maryland investigators employed facial recognition to identify a suspect in a bank robbery within an hour of the crime.[127] As a result, "[p]olice officers staked out the man's house, and he came out wearing the same clothes he was wearing in the surveillance footage . . . He was arrested."[128] The FBI took advantage of facial recognition in its investigation of the January 6 attack on the Capitol and its efforts to learn the identities of the people who participated.[129] State and local police—not just federal agen-

121. *Id.*

122. Thorin Klosowski, *Facial Recognition Is Everywhere. Here's What We Can Do About It*, N.Y. TIMES (July 15, 2020), https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/ [https://perma.cc/M6TE-RFDH].

123. *Id.*

124. Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. TIMES (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html [https://perma.cc/2Q4V-KEXT].

125. *Id.*

126. *Id.*

127. Justin Jouvenal & Spencer S. Hsu, *Facial Recognition Used to Identify Lafayette Square Protester Accused of Assault*, WASH. POST (Nov. 2, 2020), https://www.washingtonpost.com/local/legal-issues/facial-recognition-protests-lafayette-square/2020/11/02/64b03286-ec86-11ea-b4bc-3a2098fc73d4_story.html [https://perma.cc/2XPF-H8NA].

128. *Id.*

129. *Police Departments Adopting Facial Recognition Tech Amid Allegations of Wrongful Arrests*, CBS NEWS (May 16, 2021), https://www.cbsnews.com/

cies—hold that murder, assault, and robbery cases have all benefitted from the use of facial recognition.[130]

The value of facial recognition is usually tied to the idea of the common good, particularly public safety. However, it also serves individual and family needs, as facial recognition has proven to be useful in identifying people who are not suspected of wrongdoing, including murder victims and people suffering from Alzheimer's disease.[131] Furthermore, facial recognition helped investigators find a man who posted suicidal comments in a veterans' group on Facebook.[132] His name was unknown; however, using his picture, officials were able to identify him and make a counseling referral.[133]

Facial recognition is also a valuable tool in avoiding some significant errors that turn innocent people into suspects or defendants. Although eyewitness accounts are often given a lot of credence in investigations and prosecutions, research shows that eyewitness memories are very prone to errors.[134] The Innocence Project reports that "[m]istaken eyewitness identifications contributed to approximately 69% of the more than 375 wrongful convictions in the United States overturned by post-conviction DNA evidence."[135] The same is true for people who are asked to come to police stations and review mug shots in order to identify criminals whose images are available but not their identification.[136]

Patrick Grother, who tests facial recognition algorithms in his work as a computer scientist at the National Institute of Standards and Technology, points out that, although facial recognition technology is not perfect, computers are now "better than humans" at recognizing faces.[137] Thus, it seems as though facial recognition tools could reduce law enforcement's reliance on eyewitnesses, thereby helping to protect individuals from becoming suspects based on faulty memories and flawed procedures for dealing with eyewitness identifications.

---

news/facial-recognition-60-minutes-2021-05-16/ [https://perma.cc/K8AS-8H46] [hereinafter Police Department].

130. *Id.*

131. Valentino-DeVries, *supra* note 124.

132. Jouvenal & Hsu, *supra* note 127.

133. *Id.*

134. Gary Wells, *Vagaries of Memory Mean Eyewitness Testimony Isn't Perfect*, CONVERSATION (Nov. 30, 2014, 5:12 PM), https://theconversation.com/vagaries-of-memory-mean-eyewitness-testimony-isnt-perfect-34692 [https://perma.cc/H5PE-RFCQ].

135. *Eyewitness Identification Reform*, INNOCENCE PROJECT, https://innocenceproject.org/eyewitness-identification-reform/ [https://perma.cc/J84J-NQJS] (last visited Nov. 11, 2021).

136. *Id.*

137. Police Departments, *supra* note 129.

B. Arguments Against Government Use of Facial Recognition

Critics hold that public authorities use of facial recognition raises a variety of concerns, particularly regarding privacy, surveillance, and abuse, as well as issues of accuracy and bias.[138] Records show that law enforcement agencies employ facial recognition tools often in their investigations of low-level, non-violent crimes; a simple email is often all it takes to launch a search using facial recognition—no court order or warrant is required.[139] As a senior counsel at the Project on Government Oversight, Jake Laperruque, put it in 2019, "It's really a surveillance-first, ask-permission-later system . . . [S]earches are happening very frequently today. The FBI alone does 4,000 searches every month, many draw on state DMVs."[140] The government requires people to have their picture taken for driver's licenses and passports, but the people involved never agreed to provide the government with their picture for the purposes of criminal investigations.[141] Some experts "warn that the technology—which can be used to track people at a distance without their knowledge—has the potential to lead to ubiquitous surveillance, chilling freedom of movement and speech."[142]

Some suggest that the abuse of facial recognition technology has already begun. In 2019, Georgetown Law's Center on Privacy and Technology (Center) published research that revealed that police investigators input a wide variety of images into facial recognition tools, including artist sketches, low-quality stills from surveillance videos, images in which suspects' facial features are computer-generated, and celebrity lookalikes.[143] The Center discovered that "[a]t least half a dozen police departments across the country permit, if not encourage, the use of face recognition searches on forensic sketches—hand drawn or computer generated composite faces based on descriptions that a witness has offered."[144] This practice has been shown to

138. Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, WASH. POST (July 7, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/ [https://perma.cc/Z5VY-E8MD].

139. *Id.*

140. *Id.*

141. *Id.*

142. Natasha Singer & Cade Metz, *Many Facial-Recognition Systems Are Biased, Says U.S. Study*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html [https://perma.cc/J3V8-QYHA].

143. Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEORGETOWN L. CTR. ON PRIVACY & TECH., n.53 (May 16, 2019), https://www.flawedfacedata.com/ [https://perma.cc/YEW2-P4WP].

144. *Id.*

reduce the efficacy of facial recognition as an identification tool, either failing to identify any potential matches or leading to misidentification.[145]

Critics argue that facial recognition searches are problematic because public authorities are overly trusting of the technology and the mathematical computations that provide their base, assuming that the results must be accurate.[146] As Clare Garvie, a Center on Privacy and Technology lawyer and author of the 2019 report, stated, "When we want to agree with the computer, we are gonna go to find evidence that agrees with it."[147] Thus, law enforcement officials are likely to focus intently on individuals who come up in facial recognition searches, regarding them as guilty and concentrating on them to find evidence to support that assumption.

In another 2019 report, researchers at the Center discovered that Immigration and Customs Enforcement (ICE) uses facial recognition on state driver's license databases in order to find and deport undocumented immigrants.[148] Many states have passed laws allowing, and even encouraging, undocumented immigrants to obtain driver's licenses or other similar forms of identification/certification.[149] A lack of authorization from Congress and state legislatures has not deterred federal agencies from their efforts to tap into state databases.[150] Federal agencies, including ICE, have been able to rely on a law, passed before the advent of facial recognition technology, that favors Department of Motor Vehicle cooperation with law enforcement, does not require a court order or a search warrant, and allows requests for cooperation to move forward in secret.[151]

In 2019, the Government Accountability Office (GAO) reported that the FBI had access to twenty-one state databases, as well as local and federal databases, making a total of over 641 million images available for searches.[152] More recently, *New York Times* investigations into Clearview AI, a small company with "a groundbreaking facial recognition app," have found that the company provides law enforcement agencies with access to "a

145. *Id.*

146. *Id.*

147. Police Departments, *supra* note 129.

148. Bill Chappell, *ICE Uses Facial Recognition to Sift State Driver's License Records, Researchers Say*, NPR (July 8, 2019, 4:23 PM), https://www.npr.org/2019/07/08/739491857/ice-uses-facial-recognition-to-sift-state-drivers-license-records-researchers-sa [https://perma.cc/UT4E-MY26].

149. *Id.*

150. *Id.*

151. *Id.*

152. *Id.*

database of more than three billion images that Clearview claims to have scraped from Facebook, YouTube, Venmo and millions of other websites."[153]

Clearview's database adds to the alarm of critics who were already concerned about government use of facial recognition drawing on images in government data banks. Garvie, of Georgetown Law's Center on Privacy and Technology, notes, "The larger the database, the larger the risk of misidentification because of the doppelgänger effect. They're talking about a massive database of random people they've found on the internet."[154] In other words, Garvie maintains that the danger of misidentification increases with the size of the database. Additionally, there is concern because people posted photos of themselves and their friends and family online, without knowing or intending for those personal images to lead to faceprints.[155] One critic compared it to getting a haircut, only to find out later that the hairdresser used the hair left behind after the cut to obtain your DNA.[156]

In 2019, the National Institute of Standards and Technology issued a report based on tests conducted on most of the commercial facial recognition technologies that were available at that time.[157] Although several large technology companies chose not to submit their algorithms, ninety-nine developers participated, sharing 189 algorithms for facial recognition.[158] The tests showed that most of the systems were biased, with "[t]he systems falsely identif[ying] African-American and Asian faces 10 to 100 times more than Caucasian faces," and with even higher error rates occurring in searches of Native Americans.[159] There were also worse outcomes for women and older adults than for men and middle-aged adults.[160] The racial differences in the accuracy of facial recognition tools are particularly concerning to some critics, who "have argued . . .that the pervasive racial bias in policing will inevitably extend to how it [facial recognition technology] is wielded, not least

153. Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/T8WD-ZFC2].

154. *Id.*

155. Kashmir Hill, *What Happens When Our Faces Are Tracked Everywhere We Go?,* N.Y. TIMES (Mar. 18, 2021), https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html [https://perma.cc/VGW8-N5RF].

156. *Id.*

157. Singer & Metz, *supra* note 142.

158. *Id.*

159. *Id.*

160. *Id.*

because African-Americans are disproportionately represented in mug-shot databases."[161]

Three cases in which a Black man was wrongfully arrested and jailed as a result of misidentification by a facial recognition system made the news in 2020.[162] Nijeer Parks, one of the men, "spent 10 days in jail and paid around $5,000 to defend himself," and, because he had previously been incarcerated, he knew that losing at trial would mean a ten-year sentence.[163] Despite his innocence, Parks and his family briefly considered a plea deal.[164] The case against Parks was open for nearly a year, during which time he obtained proof of his alibi.[165] Still, when the case was finally dismissed, the reason given was a lack of evidence, which indicates that the government did not admit that they had the wrong man.[166]

C. Curbing Facial Recognition

In response to all the concerns raised by critics, several attempts have been made to curb the use of facial recognition by public authorities or even ban it outright. Joy Buolamwini, the leader of a Massachusetts Institute of Technology study that demonstrated the existence of disparities based on skin color and gender in the accuracy of identifications using facial recognition technology and the founder of the Algorithmic Justice League, participated in "call[s] for a nationwide moratorium on all government use of facial recognition technologies."[167]

Northeastern University law and computer science professor Woodrow Hartzog has argued:

> We've relied on industry efforts to self-police and not embrace such a risky technology, but now those dams are breaking because there is so much money on the table. I don't see a future where we harness the benefits of face recognition technology without the

161. Amy Harmon, *As Cameras Track Detroit's Residents, a Debate Ensues Over Racial Bias*, N.Y. Times (July 8, 2019), https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html [https://perma.cc/WX7B-3RX7].

162. Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. Times (Dec. 29, 2020), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html [https://perma.cc/P429-YRM4].

163. *Id.*

164. *Id.*

165. *Id.*

166. *Id.*

167. Bobby Allyn, *Amazon Halts Police Use of Its Facial Recognition Technology*, NPR (June 10, 2020, 6:59 PM), https://www.npr.org/2020/06/10/874418013/amazon-halts-police-use-of-its-facial-recognition-technology [https://perma.cc/6PDY-9MQ8].

> crippling abuse of the surveillance that comes with it. The only way to stop it is to ban it.[168]

Others suggest solutions that are less extreme. The GAO, for example, provided the FBI six recommendations to improve its use of facial recognition and to address attendant privacy concerns.[169] The GAO was particularly concerned that the FBI has not adequately tested "whether state database searches are accurate enough to support law enforcement investigations."[170] This is significant, because "[p]oorer-quality images are known to contribute to mismatches, and dim lighting, faces turned at an angle, or minimal disguises such as baseball caps or sunglasses can hamper accuracy."[171]

In 2021, Virginia joined the ranks of jurisdictions around the country that are restricting, pausing, or banning government use of facial recognition technology.[172] Virginia's law is "one of the nation's strictest controls on facial recognition software," as it "requires local law enforcement agencies to get approval from the state legislature before using any facial recognition system."[173] California, New York, Massachusetts, Oregon, New Hampshire, and Vermont all have either regulated or prohibited government use of facial recognition, as have at least twenty cities.[174] San Francisco, Minneapolis, and Portland are among the cities that have prohibited police use of facial recognition.[175] A bipartisan bill currently under consideration in the Senate seeks to put a stop to government agencies' ability to purchase access to Clearview AI, which is "one of the most popular facial recognition programs used by hundreds of police departments across the country."[176] The European Union

168. Hill, *supra* note 155.

169. Chappell, *supra* note 148.

170. *Id.*

171. Valentino-DeVries, *supra* note 124.

172. Justin Jouvenal, *Facial Recognition System Used to Identify Lafayette Square Protester to Be Halted*, WASH. POST (May 18, 2021, 4:28 PM), https://www.washingtonpost.com/local/public-safety/facial-recognition-system-halted/2021/05/18/af2d19e2-b737-11eb-a6b1-81296da0339b_story.html [https://perma.cc/3WPU-ZBDF].

173. *Id.*

174. Denise Lavoie, *Virginia Lawmakers Ban Police Use of Facial Recognition*, ASSOC. PRESS (Mar. 29, 2021), https://apnews.com/article/technology-legislature-police-law-enforcement-agencies-legislation-033d77787d4e28559f08e5e31a5cb8f7 [https://perma.cc/NP8X-EWAX].

175. Emma Peaslee, *Massachusetts Pioneers Rules for Police Use of Facial Recognition Tech*, NPR (May 7, 2021, 6:00 AM), https://www.npr.org/2021/05/07/982709480/massachusetts-pioneers-rules-for-police-use-of-facial-recognition-tech [https://perma.cc/JW49-UJ87].

176. Drew Harwell, *Senators Seek Limits on Some Facial-Recognition Use by Police, Energizing Surveillance Technology Debate*, WASH. POST (Apr. 21, 2021,

is similarly considering legislation to restrict the use of facial recognition by police.[177] Private companies are also taking action: in the wake of the murder of George Floyd and the protests against systemic racism in policing, Amazon, IBM, and Microsoft all pledged to either permanently or temporarily stop providing law enforcement agencies with facial recognition technology.[178]

D. A Third Way

Instead of banning or greatly curbing the use of facial recognition, which is a highly effective law enforcement tool, and one that can help individuals, as we have seen, the government should take two major steps to ensure the proper use of facial recognition. First of all, there is a need for a federal law that will prevent facial recognition from ever serving as sufficient evidence in itself to charge or arrest anyone. Identification based on facial recognition could only lead to additional investigation of the person identified. Currently, there are no national laws governing either the technology industry behind facial recognition or the use of the technology.[179]

Even those who advocate for government use of facial recognition, including many law enforcement agencies, recognize that the role of facial recognition in investigations must be limited. For example, in testimony before a committee in the House of Representatives in 2019, the deputy assistant director of the FBI's Criminal Justice Information Services, Kimberly Del Greco, explained that, once the results of facial recognition searches are available to the FBI's FACE Services unit, people examine them, checking the computer-generated matches against the original image.[180] Further, she asserted that the FACE Services unit "does not provide positive identification, but rather, an investigative lead."[181] At the same time, some reports indicate that local police departments do not adhere to these strictures and that people have been arrested only on the basis of facial recognition identifi-

---

3:29 PM), https://www.washingtonpost.com/technology/2021/04/21/data-surveillance-bill/ [https://perma.cc/Z9JP-JPMX].

177. Sam Schechner & Parmy Olson, *Artificial Intelligence, Facial Recognition Face Curbs in New EU Proposal*, WALL ST. J. (Apr. 21, 2021, 9:13 AM), https://www.wsj.com/articles/artificial-intelligence-facial-recognition-face-curbs-in-new-eu-proposal-11619000520 [https://perma.cc/PG2T-D9EJ].

178. Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/PUQ2-WYPE].

179. Hill, *supra* note 153; Police Departments, *supra* note 129.

180. Chappell, *supra* note 148.

181. *Id.*

cation.[182] Hence the need for a federal law, rather than leaving the matter to each jurisdiction.

The second of the two major steps needed to ensure proper use of facial recognition is that all users of the technology should be made aware of the fact that current facial recognition software and algorithms contain biases. Hence, special caution needs to be taken when facial recognition is used to identify minorities and women. These warnings will add to the motivation of the producers of facial recognition to invest more in improving their algorithms to correct for this serious flaw. The National Science Foundation should provide grants to researchers to work on these corrections, and the White House should bring together the heads of major technology companies to help to correct this serious bias.

V. CONCLUSION

Many arguments in public discourse and in the courts take the format: there is a right; this conduct or policy violates this right; it should be stopped. Others take the format: there is a national need (or public interest or common good); this or that behavior stands in the way of severing this need; it needs to be changed. Liberal communitarianism suggests that all such deliberations should start from recognizing that society must abide by two conflicting principles: the commitment to individual rights *and* to the commit to the common good; that public discourse, legislatures, and the courts must work out when one or the other must yield after they have exhausted quests to advance both simultaneously. And that in which direction to tilt depends on the ever-changing historical conditions. Liberal communitarianism ought to be viewed as drawing on a jurisprudence implicit in the Fourth Amendment distinction between reasonable and unreasonable searches.[183]

This Article focused on three new technologies, in the current condition, in which the aftereffects of the pandemic and political trauma are deeply impacting all considerations, as well as the rise in crime and domestic terrorism. An examination of end-to-end encryption suggests that it greatly encumbers the work of public authorities, but it seems too entrenched to be banned. That the additional privacy protecting measures, a strong password, can be maintained as long as a key is kept with the technology companies, rather than inserting a backdoor into all phones.

Cryptocurrencies, this Article finds, have no redeeming social merit, and are hence one of the very few technologies that should be banned outright. They are not yet as entrenched as to make such banning politically impossible.

Facial recognition is a very powerful law enforcement tool whose abuse can lead to the arrest of many innocent people, especially minorities and women. However, instead of banning it, (1) a federal law should state that

182. Police Departments, *supra* note 129.

183. Harwell, *supra* note 138.

facial recognition by itself should never suffice to arrest or charge anyone but could be used as grounds for further investigation, to making one into a suspect; (2) major efforts must be made to correct for the biases which currently plague facial recognition, but there is no reason to hold that these cannot be corrected; and (3) facial recognition can be used to advance rights, not just public safety. In total, this Article seeks to highlight that in the current condition, there are three cases in which the American society has titled too far in allowing technologies to undermine public safety and that proper treatment of these technologies can help redress this imbalance.