



Should Detection Avoidance Be Criminalized?

Wayne A. Logan¹

Accepted: 2 June 2023

© The Author(s), under exclusive licence to Springer Nature B.V. 2023

Abstract

Human nature being what it is, individuals engaging in unlawful activity will often seek to avoid having their misconduct detected by law enforcement. This article provides the first legal analysis of what are termed detection avoidance measures, and evaluates whether, and how, they should be subject to criminalization.

Keywords Detection avoidance · Criminalization · Policing · Law and technology

1 Introduction

Because would-be lawbreakers typically do not wish to be held to account, many will undertake measures to avoid having their misconduct detected by law enforcement. A drug dealer, for instance, might use a disposable “burner” cell phone to mislead police, a possessor of child pornography encryption software to hide computer files, and a burglar a facial covering or device to neutralize the gaze of surveillance cameras. Motorists also frequently engage in detection avoidance, employing a variety of measures to avoid being stopped for speeding (e.g., laser “jammers”) and drunk driving (e.g., the “Waze” cell phone app).

Notably, all of the foregoing detection avoidance measures are lawful. In this respect, they differ from many other legally prohibited detection avoidance measures, such as having a secret compartment in a vehicle,¹ or using a firearm with a silencer to mute its sound when fired,² a “Whizzinator” to defeat a drug urinalysis test,³ or a “booster” device to neutralize anti-shoplifting measures.⁴

This article seeks to lend a degree of taxonomic coherence to the broad array of detection avoidance measures available to individuals and asks whether some or

¹ John Ross, “The Crime of Having a Hidden Compartment in Your Car”, *Reason.com* (Feb. 16, 2014) (noting that California, Ohio, Georgia, Illinois, and Oregon have such laws and that several other states were considering enactment).

² See, e.g., Cal. Penal Code s. 12520 (2020); Ga. Code Ann. s. 16-11-123 (2021).

³ See, e.g., Tex. Health & Safety Code s. 481.133 (2020).

⁴ See, e.g., N.Y. Penal Law s. 170.47 (2021).

✉ Wayne A. Logan
wlogan@law.fsu.edu

¹ Florida State University College of Law, 425 West Jefferson Street, Tallahassee, FL 32306, USA

all should be criminalized. Ultimately, the article addresses a basic question: should detection avoidance measures be viewed, in the words of sociologist Gary Marx, as “courageous and inspiring expressions of the human spirit,” or as “destructive anti-social behavior proving the need for ever more stringent controls”?⁵

Support for the former view aligns with the common cultural admiration of guileful trickers,⁶ and suspicion of governmental authority more generally (in the U.S., at least).⁷ Detection avoidance can also serve as a shield against what many see as over-enforcement of the law, especially regarding minor offenses in poor and minority communities,⁸ or afford a welcome measure of “slack” in daily life.⁹ Moreover, detection avoidance measures that cloak personal identity can obstruct private and government surveillance efforts,¹⁰ including of individuals engaged in constitutionally protected speech and assembly, such as political protests.¹¹

Yet, there are also persuasive reasons for criminalizing detection avoidance. To a proponent of criminalization, detection avoidance is triply problematic: it allows the underlying illegality to occur, constitutes conscious and purposeful avoidance of personal responsibility, and amounts to government tolerance of both the illegality and the trickery used to shield it. Moreover, tolerating detection avoidance results in doctrinal inconsistency. How is it, for instance, that use of a gun silencer is criminalized, yet one can lawfully encrypt computer files to shield child pornography? Likewise, how can a burglar lawfully wear a mask, yet acquiring a mask before a burglary can serve as a basis for attempt liability?¹²

For criminal law theoreticians, detection avoidance represents untilled terrain. Although considerable scholarly attention has been paid to the criminalization of *ex post* crime cover-up activity, such as perjury, money laundering, witness intimidation, and destruction of documents,¹³ and *ex ante* inchoate criminal behavior, such as “staking out” a potential future crime scene,¹⁴ the *in-tempore* avoidance measures

⁵ Gary T. Marx, “Seeing Hazily (But Not Darkly) Through the Lens: Some Recent Empirical Studies of Surveillance Technologies”, *Law & Social Inquiry* 30(2): pp. 339–99, p. 388.

⁶ See, e.g., Lewis Hyde, *Trickster Makes This World: Mischief, Myth, and Art* (New York: Farrar, Strauss and Giroux, 1998).

⁷ Matthew M.F. Miller, “The Radical Individualism Raging Throughout America”, *Shadowland.com*. (Nov. 20, 2022), <https://www.shadowland.com/act/news-politics/a34729330/the-radical-individualism-raging-throughout-america/>.

⁸ See *infra* notes 99–102 and accompanying text.

⁹ See *infra* notes 97–98 and accompanying text.

¹⁰ See *infra* notes 107–114 and accompanying text.

¹¹ See *infra* notes 111–112 and accompanying text.

¹² See, e.g., *United States v. Moore*, 921 F.2d 207 (9th Cir.1990); *Swint v. State*, 632 S.E.2d 712 (Ga. App. 2006).

¹³ See, e.g., Stuart P. Green, “Uncovering the Cover-Up Crimes”, *American Criminal Law Review* 42(1) (2005): pp. 9–44; Erin Murphy, “Manufacturing Crime: Process, Pretext, and Criminal Justice”, *Georgetown Law Journal* 97(6) (2009): pp. 1435–507.

¹⁴ See, e.g., Larry Alexander & Kimberly Ferzan, “When Are Inchoate Crimes Culpable and Why?”, in *Crime and Culpability: A Theory of Criminal Law* (New York: Cambridge University Press, 2009), pp. 197–225; Andrew Cornford, “Inchoate Criminality”, in Larry Alexander & Kimberly Kessler Ferzan (eds.), *The Palgrave Handbook of Applied Ethics and the Criminal Law* (Springer Verlag 2019), pp. 361–82.

focused upon here have yet to be examined. The deficit is unfortunate because detection avoidance is a common undertaking and provides a rich opportunity for analysis.

This article takes a first step in filling this gap and proceeds as follows. Part 2 provides an overview of the diverse array of measures individuals employ to avoid detection of their wrongdoing.¹⁵ Part 3 examines whether detection avoidance should be criminalized, concluding that both theoretical and instrumental reasons support criminalization, although not without some caveats. Part 4 considers how policy makers might implement criminalization, focusing principally upon the options of sanctioning detection avoidance measures themselves, *simpliciter*, or, alternatively, as an adjunct to the penalization of the underlying misconduct that is sought to be concealed.

2 Detection Avoidance Measures

Detection avoidance measures perhaps figure most commonly in the automobile context. Motorists might employ laser “jammers,” lawful in the vast majority of states,¹⁶ which prevent police speed detection laser guns from identifying a car’s speed,¹⁷ or utilize “Laser Veil Stealth Coating,” which neutralizes readings of police laser speed detectors. According to the Veil Stealth website, “Veil is a nearly colorless transparent liquid acrylic which dries into a hardy, but easily removable, weather resistant film. It is designed to absorb infrared light making it more difficult for your speed to be measured.”¹⁸ Veil, the website relates, is a “countermeasure product” that “[c]an save you thousands of dollars in fines, points and higher insurance premiums.”¹⁹ A website selling Veil, RadarBusters.com, boasts that Veil coating “transforms your radar detector from a ticket notifier into a ticket preventer...”²⁰ Veil also offers reflective or retractable license plate covers that obscure plates from detection by speed and red light cameras.²¹ Less tech-oriented motorists might use a

¹⁵ The discussion focuses in particular on the use of devices to avoid detection, not behaviors alone, such as flight from a crime scene or hiding from police, providing an initial attempt at laying the foundation for analysis of increasingly sophisticated technological detection avoidance devices to come.

¹⁶ Vortex, “Are Laser Jammers Illegal or Legal in the USA?”, Nov. 7, 2017, <https://www.vortexradar.com/2017/11/are-laser-jammers-illegal-or-legal-in-the-usa-laser-jammer-laws/> (noting that laser jammers are banned in nine states and the District of Columbia).

¹⁷ Laser jammers differ from radar jammers, which emit radio frequency signals that hide vehicle speed from a police speed detection radar or provide false radar information, which can affect airplane and air traffic control, and are therefore prohibited by federal law. 7 USC s. 333 (2020). Rocky Mountain Radar sells laser and radar “scramblers” emitting information that confounds the ability of police to determine an accurate rate of a vehicle’s speed, which purportedly avoid being characterized as illegal radar jammers. See <https://rockymountainradar.com/>.

¹⁸ <https://veilstealth.com/>.

¹⁹ <https://veilstealth.com/blogs/news>.

²⁰ <https://www.radarbusters.com/Laser-Veil-G6-Stealth-Coating-Review-p/veil.htm>.

²¹ <https://veilstealth.com/>.

mask to defeat automated cameras designed to detect the running of red lights²² and air fresheners to obscure the aroma of marijuana or other drugs.²³

Cellphone apps provide motorists several ways to avoid detection. The “Waze” app, for example, utilizes crowdsourcing to provide information indicating where police speed traps are located, so they can be avoided, allowing drivers to maintain their unlawful speed.²⁴ According to the VortexRadar website, “Waze is an excellent addition to laser jammers. It’s not a replacement for them, but it is an effective additional layer of protection to add to your countermeasure kit.”²⁵ Waze also provides information on the location of police drunk driving checkpoints.²⁶ And the NYCSpeedCamBuster app provides crowdsourced information on the location of the several hundred speed detection and red light-running cameras operative in New York City.²⁷

Outside the auto context, individuals wishing to avoid detection have a multitude of measures at their disposal. Lasers, for instance, might be used by shoplifters to defeat store security cameras²⁸; masks²⁹ or a “privacy visor”³⁰ to thwart facial recognition; a “burner” cell phone to avoid police monitoring³¹; a cell phone app³² or GPS “spoofers”

²² Brad Tuttle, “Big Brother Backlash: Citizens Unite to Bring Down Ticket-Generating Red-Light Cameras”, *Time Magazine* (Feb. 16, 2012), <http://business.time.com/2012/02/16/big-brother-backlash-citizens-unite-to-bring-downticket-generating-red-light-cameras/>.

²³ See, e.g., *United States v. Bailey*, 505 F. Supp. 3d 481 (E.D. Penn. 2020).

²⁴ Other apps include “Mr. Checkpoint,” “Checkpoint Wingman,” “Sobriety Alerts,” “DUI Savor,” and “Phantom ALERT.” As discussed later, there will likely be occasions, admittedly rare, when a driver will use the information to slow down to a lawful speed for the duration of a trip.

²⁵ <https://www.vortexradar.com>. The widely used “Trapster” app, which provided real time location information on police speed traps, DUI checkpoints, red light cameras, and speed cameras, operated until 2014.

²⁶ To date, Google has resisted law enforcement demands that the Waze information be removed. Michal Gold, “Police Demand That Waze App Stop Tipping Drivers Off to Checkpoints”, *N.Y. Times* (Feb. 6, 2019), p. A23, <https://www.nytimes.com/2019/02/06/nyregion/waze-nypd-location.html>. New York City police stated that posting the information was “irresponsible since it only serves to aid impaired and intoxicated drivers to evade checkpoints and encourage reckless driving. Revealing the location of checkpoints puts those drivers, their passengers, and the general public at risk.” According to a National Sheriff’s Association spokesperson, “[u]sing crowdsourcing doesn’t stop you from breaking the law. It just allows you to be prevented from being arrested. That’s a direct undermining of the rule of law.” *Ibid*.

²⁷ Eve Kessler, “New App Helps Reckless Drivers Thumb Their Noses at City’s Speed Cameras”, *Streetsblog NYC* (May 13, 2002), <https://nyc.streetsblog.org/2022/05/13/new-app-helps-reckless-drivers-thumb-their-noses-at-citys-speed-cameras/>.

²⁸ John Markoff, “Protesting the Big Brother Lens, Little Brother Turns an Eye Blind”, *N.Y. Times* (Oct. 7, 2002), p. C1, <https://www.nytimes.com/2002/10/07/business/protesting-the-big-brother-lens-little-brother-turns-an-eye-blind.html>.

²⁹ Jesse Emspak, “How to Beat Facial Recognition Software”, *NBC News*, http://www.nbcnews.com/id/46153896/ns/technology_and_science-security/#Un-nPPnYeSo (last updated Jan. 26, 2012, 4:49 PM).

³⁰ Tim Hornyak, “Foil Face-Recognition Cameras with Privacy Visor”, *Cnet.com* (Jan. 22, 2013), <https://www.cnet.com/culture/foil-face-recognition-cameras-with-privacy-visor/>.

³¹ See, e.g., *Commonwealth v. Shields*, 258 A.3d 509 (Pa. 2021).

³² Rob Pegoraro, “How to Block—or Blur—Your Location from Your Smartphone’s Apps”, *USA Today* (July 1, 2022), <https://www.usatoday.com/story/tech/columnists/2022/07/01/how-to-hide-location-phone-steps/7784274001/>.

to thwart geo-location tracking³³; and a jammer to neutralize the gaze of wireless home surveillance cameras.³⁴ An individual can also disguise their voice to confound voice detection technology,³⁵ and encrypt computer files to conceal child pornography.³⁶

Individuals seeking to avoid detection of unlawful substances in their urine engage in what qualifies as the most unusual strategy surveyed here. A “Whizzinator,” its manufacturer explains on its website, is

a fake penis made from a rubbery plastic that comes with an attached reservoir for holding a clean or synthetic urine sample. Both the prosthetic appendage and urine reservoir are attached to an elastic belt worn under the clothing. While providing the sample, the wearer pulls the Whizzinator out of their underwear, and then they activate a valve (silently and with one hand using the improved Whizzinator Touch!) to release the urine, which flows out of the fake penis and into the sample cup.³⁷

Looking ahead, a variety of technological advances will augment the detection avoidance arsenal. To counter efforts to monitor phone conversations, we will have “neck audio cloaks” that “take the form of a hat that rains down white noise thwarting any possibility of recording someone’s chatter.”³⁸ To avoid drone surveillance, “stealth wear” will include an “an anti-drone hoodie and scarf that are designed to thwart the thermal-imaging technology widely used by [drones].”³⁹ And the list continues to grow by the day.⁴⁰

³³ David Hambling, “GPS Signals Now Help You Call Your Mother, Power Your Home, and Even Land Your Plane...But a Cheap Plastic Box Can Jam It All”, *New Scientist* (Mar. 12, 2011), p. 44, <https://www.newscientist.com/article/dn20202-gps-chaos-how-a-30-box-can-jam-your-life/>.

³⁴ Kiara Hay, “How Criminals Are Using Jammers, Deauthers to Disrupt WiFi Security Cameras”, *WXYZ.com* (ABC Detroit) (Sept. 6, 2022), <https://www.wxyz.com/news/how-criminals-are-using-jammers-deauthers-to-disrupt-wifi-security-cameras>.

³⁵ Simon Hill & Paul Beaton, “The Best Voice-Changing Apps for Android and iOS”, *DigitalTrends.com* (Apr. 8, 2022), <https://www.digitaltrends.com/mobile/best-voice-changer-apps/>.

³⁶ See, e.g., *United States v. Wauguespack*, 935 F.3d 322 (5th Cir. 2019).

³⁷ <https://merryjane.com/culture/what-is-the-whizzinator-and-can-it-actually-beat-drug-tests>.

³⁸ Nick Bilton, “Shields for Privacy in a Smartphone World”, *N.Y. Times* (June 25, 2012), p. B5.

³⁹ Tim Maly, “Anti-Drone Camouflage: What to Wear in Total Surveillance”, *Wired* (Jan. 17, 2013, 3:14 PM), <http://www.wired.com/design/2013/01/anti-drone-camouflage-apparel/>. See also <https://ahprojects.com/stealth-wear/>.

⁴⁰ See, e.g., Aaron Holmes, “These Clothes Use Outlandish Designs to Trick Facial Recognition Software into Thinking You’re Not Human”, *Business Insider* (June 5, 2020), <https://www.businessinsider.com/clothes-accessories-that-outsmart-facial-recognition-tech-2019-10>.

3 Should Detection Avoidance Be Criminalized?

This part turns from the descriptive to the normative, considering the arguable wrongfulness and harmfulness of detection avoidance,⁴¹ baseline prerequisites for criminalization,⁴² as well as several broader instrumental considerations.

3.1 The Case for Criminalization

Wrongfulness, of course, can be defined in any number of ways. Viewed in terms of one common understanding, detection avoidance is wrong because the unlawful activity avoiders engage in, and seek to evade accountability for, transgresses a democratically enacted norm of a polity.⁴³ One might well disagree with auto speed limits, for instance, but the limits come within what Antony Duff calls “regulations that [individuals] ought to obey if they help maintain the efficient workings of systems that serve the common good; we do wrong when we breach them.”⁴⁴ Because detection avoidance (when successful) both enables the unlawful activity to occur

⁴¹ The arguments favoring criminalization apply trans substantively, regardless of the nature and severity of the underlying offense that eludes detection, *malum prohibitum*, *malum in se*, or hybrid. As discussed later, policy makers might tie punishment for detection avoidance to the seriousness of the underlying offense.

⁴² See, e.g., Stuart P. Green, *Lying, Cheating, and Stealing: A Moral Theory of White-Collar Crime* (Oxford and New York: Oxford University Press, 2006), pp. 42–43 (identifying harm to others and wrongfulness as core attributes of a crime). There has been a debate of course over whether all wrongdoing, including of a personal moral nature (such as lying) should be criminalized, as largely maintained by Michael Moore, in *Placing Blame* (1998), or whether only public wrongs should be criminalized, as maintained by Antony Duff and others. See, e.g., R.A. Duff, *The Realm of Criminal Law* (Oxford: Oxford University Press, 2018), p. 274 (stating that “we have good reason to criminalize conduct if and only if it constitutes a public wrong; and conduct constitutes a public wrong if and only if it violates the polity’s civil order.”). The latter view is adopted here.

⁴³ See, e.g., R.A. Duff, “Criminal Law and the Constitution of Civil Order”, *University of Toronto Law Journal* 70(Supp. 1) (2020): pp. 4–26, p. 15 (asserting that “criminal law is not concerned with moral wrongs as such...but only with ‘public’ wrongs. And what makes a wrong public...is not some inherent characteristic of the wrong itself or the fact that it has some adverse consequential impact on ‘the public’, but that it falls within, or impinges upon, the public realm that is defined by the polity’s civil order.”); *ibid.* p. 16 n.45 (“To assume that [criminal laws] have a legitimate claim on our obedience is not to rely on a general obligation to obey the law; it is to assume that the regulations can be justified as good faith attempts to serve the common good.”). For similar accounts, see, e.g., Vincent Chiao, “What Is the Criminal Law For?”, *Law and Philosophy* 35 (2016): pp. 137–63, p. 139; Harold L. Korn, “The Choice-of-Law Revolution: A Critique”, *Columbia Law Review* 83 (1983): pp. 772–973, p. 799; Malcolm Thornburn, “Criminal Punishment and the Right to Rule”, *University of Toronto Law Journal* 70(Supp. 1) (2020): pp. 44–63, p. 31. The arguable exception of “situational” wrongdoers, those having principled objection to a law, is discussed later.

⁴⁴ R.A. Duff, *Answering for Crime: Responsibility and Liability in the Criminal Law* (Oxford: Hart Publishing, 2007), p. 174. See also Duff, “Civil Order”, p. 16 (stating that “[a]ssuming (as the law must) that such regulations have a legitimate claim on our obedience, we do wrong if we break them, and the criminal law, in making it an offense to break these regulations, declares that wrong to be a public wrong”).

and evasion of accountability for it, it qualifies as what Larry Alexander and Kim Ferzan term “scofflaw” behavior, a proper subject of criminalization.⁴⁵

From a behavioral ethics perspective, detection avoiders are not “erroneous” wrongdoers unaware that they are engaged in wrongdoing.⁴⁶ Rather, they embody Holmes’ proverbial “bad man”⁴⁷: they are calculating individuals who deliberately engage in wrongful behavior,⁴⁸ and opportunistically seek to avoid legal accountability when doing so,⁴⁹ much like those engaging in already criminalized *ex post* detection avoidance behavior that frustrates the ability of government to apprehend wrongdoers (e.g., money laundering).⁵⁰ By refusing to play by the rules, detection avoiders flout basic notions of reciprocal fair play and equal treatment,⁵¹

⁴⁵ Larry Alexander & Kimberly K. Ferzan, *Reflections on Crime and Culpability: Problems and Puzzles* (Cambridge: Cambridge University Press, 2018), p. 85.

⁴⁶ See Yuval Feldman, *The Law of Good People: Challenging States’ Ability to Regulate Human Behavior* (Cambridge: Cambridge University Press, 2018), pp. 311–13. Although beyond the scope of coverage here, which focuses on the use of devices rather than behaviors, there is the question of whether providing information used by others to avoid police detection—for instance, those who contribute information to the Waze app regarding the location of police drunk driving checkpoints—should be subject to criminal sanction. Arguably, the information providers are accomplices, a common basis for criminal liability. *Model Penal Code* s. 2.06(3)(a)(ii). However, the liability of information providers can be complicated by First Amendment free speech concerns. On the issue more generally see Eugene Volokh, “Crime-Facilitating Speech”, *Stanford Law Review* 57 (2005): pp. 1095–222.

⁴⁷ Oliver Wendell Holmes, “The Path of the Law”, *Harvard Law Review* 10(8) (1897): pp. 457–78, pp. 459–61.

⁴⁸ In some instances, individuals might be “situational” wrongdoers, who harbor a principled objection to a legal norm. Feldman, *The Law of Good People*, p. 61. Insofar as this is the case, such individuals, it is submitted, should follow the time-honored tradition of civil disobedience, whereby one overtly (not covertly) violates a law to achieve its transformation. The same can be said for disagreement with silly or outmoded laws, such as Sunday “blue laws.” On civil disobedience more generally see Kimberley Brownlee, “The Communicative Aspects of Civil Disobedience and Lawful Punishment”, *Criminal Law and Philosophy*, 1(2) (2007): pp. 179–92. Detection avoiders, who employ deceit to avoid legal accountability, are the antithesis of those engaging in overt acts of civil disobedience.

⁴⁹ See Chiao, “What Is Criminal Law For?”, p. 138 (“By attaching sanctions to willful noncompliance with a legal rule, the criminal law provides assurance that the reward for cooperation will not be opportunistic defection.”).

⁵⁰ Thanks to Stuart Green for this observation. See also Youngjae Lee, “Mala Prohibita, The Wrongfulness Constraint, and the Problem of Overcriminalization”, *Law and Philosophy* 41(2022): pp. 375–96, pp. 393–94 (discussing current criminalization of activity intended to “frustrate the government’s efforts to enforce its laws through apprehension,” such as money laundering, destruction of evidence, and flight from a jurisdiction to avoid prosecution or provide testimony).

⁵¹ See Douglas Husak, *Overcriminalization: The Limits of the Criminal Law* (New York: Oxford University Press, 2008), pp. 116–17; Richard Dagger, “Authority, Legitimacy, and the Obligation to Obey the Law”, *Legal Theory* 24(2) (2018): pp. 77–102; H.L.A. Hart, “Are There Any Natural Rights?”, *The Philosophical Review* 64(2) (1955): pp. 175–91; John Rawls, “Obligations and the Duty of Fair Play”, in S. Hook (ed.), *Law and Philosophy* (New York: New York University Press, 1964), p. 3. See also Robert Nozick, *Anarchy, State, and Utopia* (New York: Basic Books, 1974), p. 90 (saying of the principle of fairness that in a cooperative society wherein individuals “restrain their liberty in ways necessary to yield advantages for all, those who have submitted to these restrictions have a right to similar acquiescence on the part of those who have benefited from their submission”).

exhibiting what Duff calls “civic arrogance.”⁵² They “unfairly exploit[] the law abidingness of their fellow citizens,”⁵³ effectively treating them as suckers.⁵⁴

Detection avoidance also imposes harm. As noted at the outset, detection avoidance is harmful because it undermines the even-handed rule of law,⁵⁵ which as Alexander and Ferzan note is “a legally recognized harm” in itself.⁵⁶ Individuals successfully using avoidance measures will avoid police detection of their misconduct, while those abstaining will not, and will suffer the adverse consequences. This disparity in treatment, and the free ridership it entails,⁵⁷ imposes a harm regardless of whether non-detection avoiders and government authorities are aware of the successful detection avoidance.

When the detection avoidance is known, and goes unsanctioned by government, however, there can come an additional harm: the potential fostering of social resentment and disillusionment with rule compliance more generally.⁵⁸ One might justifiably ask “why should I play by the rules, when I can act like others and avoid being held accountable for violating them?”⁵⁹ In such an environment, “contagious”

⁵² R.A. Duff, “Crime, Prohibition, and Punishment”, *Journal of Applied Philosophy* (19)(2) (2002): pp. 97–108, 104.

⁵³ *Id.* See also Duff, *Answering for Crime*, p. 171 (regarding conscious wrongdoing as a “denial of civic fellowship” and averring “a recognition of fellow citizenship...should motivate me to [be law-abiding]... [A]s long as the demands the law makes on me are not onerous, I ought to accept this modest burden as an implication and expression of citizenship”).

⁵⁴ See N.J. Schweitzer, Douglas J. Sylvester, & Michael J. Saks, “Rule Violations and the Rule of Law: A Factorial Survey of Public Attitudes”, *DePaul Law Review* 56 (2007): pp. 615–38, p. 632 (discussing social science findings showing strong public consensus on the importance of rule obedience).

⁵⁵ Antonin Scalia, “The Rule of Law as a Law of Rules”, *University of Chicago Law Review* 56 (1989): pp. 1175–88, p. 1178.

⁵⁶ Alexander & Ferzan, *Reflections on Crime and Culpability*, p. 313.

⁵⁷ See *ibid.* (noting that lawbreakers free ride “on the restraint of others”: they “receive[] a benefit from others’ restraint while failing to abide by the [collective’s] agreement.”). See also John Rawls, *A Theory of Justice* (Cambridge, Mass.: Harvard University Press, 1971, revised edition, 1999), p. 96 (“when a number of persons engage in a mutually advantageous cooperative venture according to rules, and thus restrict their liberty in ways necessary to yield advantages for all, those who have submitted to these restrictions have a right to a similar acquiescence on the part of those who have benefitted from their submission. We are not to gain from the cooperative labors of others without doing our fair share.”).

⁵⁸ See Stuart P. Green, “Why It’s a Crime to Tear the Tag Off a Mattress: Overcriminalization and the Moral Content of Regulatory Offenses”, *Emory Law Journal* 46 (1997): pp. 1553–615, p. 1612 (noting that tolerated law-breaking causes “damage to the authority of the government; a lessening of the public’s confidence in our institutions; public cynicism, fear, and uncertainty; and a social climate that is likely to lead to even greater disobedience”). See also Andrew Cornford, “Rethinking the Wrongness Constraint on Criminalization”, *Law and Philosophy* 36 (2017): pp. 615–49, p. 646 (noting that non-compliance with laws “tends to endanger the system itself—and correspondingly, to erode citizens’ confidence that others will comply with the relevant rules”). Whether social harm actually results from the law violated is beyond the scope of this paper. Drunk driving that causes no personal or property harm is one contested example. Youngjae Lee, “Mala Prohibita and Proportionality”, *Criminal Law and Philosophy* 15 (2021): pp. 425–46, p. 434.

⁵⁹ See Brent Fisse, “Reconstructing Corporate Criminal Law: Deterrence, Retribution, Fault, and Sanctions”, *Southern California Law Review* 56 (1983): pp. 1141–226, p. 1178 n.163 (“One should remember...that the deliberate or reckless violation of law itself creates resentment.”).

A recent occurrence illustrates how detection avoidance can motivate vigilante efforts by others. See Corey Kilgannon, “They Dispense Street Justice, One Defaced License Plate at a Time”, *N.Y. Times* (Dec. 17, 2022) (discussing efforts by community members to modify car license plates, which have been purposefully defaced or obscured by car owners, to allow them to be held accountable by cameras enforcing traffic laws and tolls evaded by owners), <https://www.nytimes.com/2022/12/17/nyregion/license-plate-vigilantes.html?smid=nytcore-ios-share&referrerSource=articleShare>.

copycat behaviors will have appeal, further undermining the rule of law.⁶⁰ Exacerbating matters, when detection avoidance depends on one's economic wherewithal to obtain a detection avoidance device, those with economic means will be able to avoid liability, while those without it will not.⁶¹ Individuals in the former group will enjoy an unfair advantage,⁶² another potential source for harmful social resentment.⁶³

Detection avoidance is also problematic for instrumental reasons.⁶⁴ In communicative and expressive terms, failure to sanction detection avoidance implicitly condones law breaking and the evasion of personal accountability that it allows. Criminalization singles out detection avoidance for condemnation,⁶⁵ which decreases the risk of public disillusionment associated with the perceived uneven enforcement of the law, which can lessen law abidingness and public willingness to help in the maintenance of public order.⁶⁶

Another instrumental consideration—whether criminalization will actually reduce detection avoidance, and possibly the underlying behavior it seeks to

⁶⁰ See Hadar Dancig Rosenberg & Yuval Feldman, "A Behavioral Ethics Perspective on the Theory of Criminal Law & Punishment", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4222232 (attaching importance to the "contagiousness" of misconduct when assessing its anti-social significance). Conversely, if the avoidance behavior goes unobserved by community members, it is not susceptible of social condemnation, increasing the reason for criminalization. Cf. Duff, *The Realm of Criminal Law*, pp. 280–81 (using queue jumping as an example of a public wrong that can be regulated informally, by public condemnation, without the intervention of the criminal law).

⁶¹ For instance, radar detectors, which allow drivers to slow down when police radar is present and thereafter violate speed limits when it is not, can cost over \$500. Hearst Autos Gear Team, "8 Top-Rated Radar Detectors for Speed Demons", Autoweek.com (Feb. 16, 2021), <https://www.autoweek.com/gear/g35492827/top-rated-radar-detectors-for-speed-demons/>.

⁶² See Michael Davis, "Why Attempts Deserve Less Punishment Than Complete Crimes", *Law and Philosophy* 5(1) (1986): pp. 1–32, pp. 11–12 ("The advantage of lawbreaking is the advantage one gets by a certain sort of cheating...One takes some of the fruits of social cooperation one is not entitled to while depending on others not to do the same.").

⁶³ Federal courts, when considering whether government use of malware on defendants' computers is a Fourth Amendment search, have spoken to this concern. See *United States v. Werdene*, 188 F. Supp. 3d 431, 446 (E.D. Pa. 2016) (the defendant should not "serendipitously receive Fourth Amendment protection because he used Tor in an effort to evade detection"); *United States v. Acevedo-Lemus*, No. SACR 15–00137-CJC, 2016 WL 4208436, at *6 (C.D. Cal. Aug. 8, 2016) (the defendant should not be allowed to "conceal his deviant behavior through Internet tricks").

⁶⁴ See R.A. Duff, "Towards a Modest Legal Moralism", *Criminal Law and Philosophy* 8(1) (2014): pp. 217–35, p. 226 (recognizing that "[i]t would be absurd to deny that instrumentalist considerations are relevant to criminalization: attention to the likely effects of criminalizing (or of not criminalizing), and of this or that particular mode of criminalization, is crucial to final decisions about whether, and how, to criminalize.").

⁶⁵ On the communicative and expressive functions of the criminal law more generally see Dan Markel, "Retributive Justice and the Demands of Democratic Citizenship", *Virginia Journal of Criminal Law* 1 (2012): pp. 1–133, at p. 26, notes 65 & 66. See also Cornford, "Rethinking the Wrongness Constraint on Criminalization", p. 648 ("To criminalize conduct is to facilitate its condemnation and punishment; to coerce citizens against it; and to portray it as wrongful.").

⁶⁶ See generally Tom R. Tyler, *Why People Obey the Law* (Princeton: Princeton University Press, 2006); Tom R. Tyler & Jeffrey Fagan, "Legitimacy and Cooperation: Why Do People Help the Police Fight Crime in Their Communities?" *Ohio State Journal of Criminal Law* 6 (2008): pp. 231–75.

hide—is a question of obvious importance.⁶⁷ Some insights are found in a small but significant pocket of the economic analysis of crime literature.

Although the field initially ignored detection avoidance,⁶⁸ later work has taken it into consideration.⁶⁹ A foremost scholar in the field today is Chris Sanchirico, who has advanced a “detection avoidance principle”: that the threat of detection and punishment not only potentially discourages a legal violation, but “also encourages those who still commit the violation to expend additional resources avoiding detection.”⁷⁰ Sanchirico posits that “violators are more than mere spectators. Just as the state invests in detecting their violations, they invest in avoiding that detection.”⁷¹

To disrupt this dynamic, Sanchirico advocates sanctioning detection avoidance with “second-order sanctions” as a way to increase deterrence of the underlying violation.⁷² He recognizes, however, that the matter is complicated by the fact that sanctioning detection avoidance possibly “generates additional effort to avoid detection of the [detection avoidance] activity.”⁷³ Because of this recursiveness, uniformly sanctioning detection avoidance is “likely to increase, not decrease, detection avoidance” over time.⁷⁴ Furthermore, Sanchirico reasons, the successive sanctioning “that would be required to reduce detection avoidance” would be “impractical.”⁷⁵

⁶⁷ On the connection between the communicative effect of criminalization and deterrence of criminal activity see Apel, “Sanctions, Perceptions, and Crime”, p. 206 (recognizing that deterrence is “rooted in coercive communication about the consequences of crime....[D]eterrence is a mechanism of information transmission and not merely a sanctioning system.”).

⁶⁸ See Gary S. Becker, “Crime and Punishment: An Economic Approach”, *Journal of Political Economy* 76(2) (1968): pp. 169–217, 176.

⁶⁹ For perhaps the first such effort, recognizing the error of Becker’s premise that optimal fines are always those set as high as possible, because doing so possibly incentivizes detection avoidance efforts, see Arun S. Malik, “Avoidance, Screening, and Optimum Enforcement”, *RAND Journal of Economics* 21(3) (1990): pp. 341–53.

⁷⁰ Chris W. Sanchirico, “Detection Avoidance and Enforcement Theory”, in 8 *Encyclopedia of Law and Economics: Procedural Law and Economics* (Cheltenham, UK: Edward Elgar Publishing, 2nd ed., 2012), p. 145, p. 155 [hereinafter Enforcement Theory].

⁷¹ *Ibid.*, p. 156.

⁷² *Ibid.*, p. 153. Sanchirico notes that other scholars assumed that sanctioning detection avoidance is not possible because the measures are unobservable by law enforcement. The empirical assumption is incorrect, as he properly notes with respect to *ex post* avoidance measures such as witness intimidation and perjury, which are detectable. More pertinent to the discussion here, police can observe many detection avoidance measures such as encryption and facial disguises.

⁷³ *Ibid.* at 170. Sanchirico elaborates: “The recursivity of detection avoidance thus spins out a potentially infinite sequence of ever greater orders of detection avoidance. Sanctioning the underlying offense encourages ‘first-order’ detection avoidance. Sanctioning first order detection avoidance encourages ‘second-order’ detection avoidance. Sanctioning second-order detection avoidance encourages third-order. Sanctioning third encourages fourth and so on.”

⁷⁴ *Ibid.*

⁷⁵ *Ibid.*, pp. 174 & 178. See also Chris W. Sanchirico, “Detection Avoidance”, *New York University Law Review* 81 (2006): pp. 1331–99, p. 1339 [hereinafter Detection Avoidance] (reasoning that sanctioning *ex post* evidentiary cover-up misconduct, such as perjury, “makes covering up the cover-up more imperative”). Ultimately, in lieu of sanctioning detection avoidance, Sanchirico suggests a “technological approach” whereby “public detection spending [is] specially changed so that each dollar and each unit of effort spent avoiding detection buys less of a reduction in the probability of detection.” *Ibid.*, p. 1337.

Two other prominent scholars in the field, Jacob Nussim and Avraham Tabbach, view individuals' investment of resources in detection avoidance as socially wasteful, and therefore think it desirable to curtail it.⁷⁶ They contend that while *ex ante* regulation of detection avoidance (e.g., taxing the sale of radar detectors) will decrease both avoidance and crime, *ex post* punishment (e.g., increasing fines for being caught for speeding with a detector) can be counterproductive insofar as it likely begets more avoidance and more crime.⁷⁷ This is because *ex post* punishment “increases not only the (marginal) costs but also the (marginal) benefits of investing in avoidance, because avoidance and crime are generally complements,”⁷⁸ in that “increased crime leads to greater avoidance, and vice versa.”⁷⁹ In sum, Nussim and Tabbach write, *ex ante* regulation is superior to *ex post* punishment because it:

necessarily deters both avoidance and crime, while *ex post* punishment does not. *Ex post* punishment of avoidance is usually simpler to implement, but counter-intuitively it may undermine deterrence of both avoidance and crime. This is because it increases both the costs and benefits of avoidance.⁸⁰

The scholarship summarized above yields some important insights. Logically, the greater the threatened punishment for the underlying misconduct, the greater the incentive to avoid detection (especially if it is low cost). And, logically, efforts to avoid detection might well inspire recursive, cat-and-mouse activity between individuals augmenting their detection avoidance measures⁸¹ and police ratcheting up their detection efforts (as we now see when encryption by individuals prompts police “workarounds”⁸² and hacking⁸³).

However, as with much of the economic analysis of crime literature more generally, with its focus on social cost and the optimal fines needed to deter rational actors, the scholarship concerning detection avoidance is not altogether helpful here.⁸⁴ Most significantly, by focusing exclusively on deterrence, the literature

⁷⁶ Jacob Nussim & Avraham D. Tabbach, “Controlling Avoidance: Ex Ante Regulation Versus Ex Post Punishment”, *Review of Law and Economics* 4(1) (2008): pp. 45–63, 47 [hereinafter Controlling Avoidance].

⁷⁷ *Ibid.*, p. 46.

⁷⁸ *Ibid.*

⁷⁹ Jacob Nussim & Avraham D. Tabbach, “Deterrence and Avoidance”, *International Review of Law and Economics* 29 (2009): pp. 314–23, p. 321 [hereinafter “Deterrence and Avoidance”].

⁸⁰ Nussim & Tabbach, “Controlling Avoidance”, p. 62.

⁸¹ Predictably, businesses will eagerly aid in these efforts. See, e.g., Bilton, “Shields for Privacy in a Smartphone World” (noting that “companies...have an incentive to create technologies that protect citizens from their government and deter officials from documenting our every move”).

⁸² Orin S. Kerr & Bruce Schneider, “Encryption Workarounds”, *Georgetown Law Journal* 106 (2018): pp. 989–1018.

⁸³ Jonathan Mayer, “Government Hacking”, *Yale Law Journal* 127 (2018): pp. 570–662. Cf. Jonathan James & Eric Beuregard, “Murderer v. Investigator: Factors Influencing the Resolution of Sexual Homicide Cases”, *Police Practice & Research* 21(2) (2020): pp. 172–86 (discussing investigating methods police use to counteract detection avoidance measures employed by individuals committing sexual homicides).

⁸⁴ A notable exception is found in Avraham D. Tabbach, “The Social Desirability of Punishment Avoidance”, *Journal of Law, Economics, & Organization* 26 (2007): pp. 265–89, which takes account of imprisonment as a penal sanction. According to Tabbach: “Avoidance efforts are socially costly because

disregards desert, a cornerstone of the preceding normative analysis.⁸⁵ Moreover, on the merits, the theoretical modeling ignores two important empirical realities. The first, long recognized by criminologists,⁸⁶ and only recently considered by economic analysis of crime scholars more generally,⁸⁷ is that would-be offenders vary in their awareness of and sensitivity for risk of apprehension. Second, relatedly, the models fail to account for variation in actors' degrees of sophistication when engaging in criminal activity, for instance regarding police wherewithal to collect forensic evidence, another empirical reality recognized by criminologists.⁸⁸

Yet, even on their own terms, the detection avoidance economic models are problematic. By regarding detection avoidance measures as a discrete "cost" (for expenses incurred), and part of the "effective sanction of the underlying violation" an actor potentially faces,⁸⁹ the literature elides the reality that many measures are very low cost (e.g., wearing a mask or using Veil spray on a license plate).⁹⁰ And, even with relatively costly measures, such as a "privacy visor" or radar detector, the financial outlays are likely far less than those associated with the measures Sanchirico focuses upon, post-offense "evidentiary misconduct" such as suborning perjury by a witness and document destruction. Meanwhile, Nussim and Tabach's model might be practical with the example of radar detectors they use, but it is not practical with items not solely intended to avoid detection (i.e., dual-use items such as masks, discussed below).⁹¹ Finally, while the models properly take

Footnote 84 (continued)

they waste real resources and reduce the expected punishment, thereby increasing the enforcement costs of achieving deterrence. However, since avoidance efforts are also costly to offenders, they may substitute for socially costlier sanctions, such as imprisonment, thereby saving punishment costs. This benefit of avoidance may outweigh its social costs, suggesting that avoidance should not necessarily be discouraged." *Ibid.*, p. 281. *See also ibid.*, p. 266 ("[I]f sanctions are socially costly over and above the costs incurred by the offenders, as is generally the case with imprisonment, then avoidance efforts may confer a social benefit by reducing punishment costs that might outweigh their social costs. Since avoidance efforts are also costly to offenders, they may substitute for socially costlier punishments.").

⁸⁵ For elaboration on why economic analysis fails to provide an ample basis for an informed theory of criminalization, especially regarding utilitarian considerations, see Husak, *Overcriminalization.*, p. 188 n.44 (noting that "a utilitarian theory of criminalization is importantly dissimilar from economic analysis. The latter seeks to prohibit inefficient acts of market bypassing no matter how much utility may be created by the transfer").

⁸⁶ *See, e.g.*, Robert Apel, "Sanctions, Perceptions, and Crime", *Annual Review of Criminology* 5 (2022): pp. 205–27.

⁸⁷ *See, e.g.*, Berno Buechel, Eberhard Feess, & Gerd Muehlheusser, "Optimal Law Enforcement with Sophisticated and Naïve Offenders", *Journal of Economic Behavior & Organization* 177 (2020): pp. 836–57.

⁸⁸ *See, e.g.*, Claire Ferguson, *Detection Avoidance in Homicides: Debates, Explanations and Responses* (London and New York: Routledge, 2021); Julien Chopin & Eric Beauregard, "Sex Offenders' Forensic Awareness Strategies to Avoid Police Detection", in Bryanna Fox, Joan A. Reid, & Anthony J. Masy (eds.), *Science Involved Policing* (Cham, Switzerland: Springer Publishing, 2020).

⁸⁹ Sanchirico, "Enforcement Theory", p. 154.

⁹⁰ *See also, e.g.*, Richard Willing, "Criminals Try to Outwit DNA", *USA Today* (Aug. 28, 2000) (noting "sinister creativity" of criminals and discussing use of masks, gloves, and plastic-covered shoes).

⁹¹ A subtle but important issue also overlooked is that the device purchased itself might increase likelihood of punishment when detected. *See, e.g.*, Brady Klopfer, "Radar Detector Rules for All 50 States" (Sept. 2, 2016), <https://www.yourmechanic.com/article/radar-detector-rules-for-all-50-states-by-brady-klopfer> (noting that "the only downside is that if you get caught with a radar detector, your chances of

account of the likely recursive nature of detection avoidance measures, they fail to recognize that an actor might utilize more than one strategy when avoiding detection of a single crime.

3.2 Caveats

Criminalizing detection avoidance is not without complication. One concern is that a detection avoidance measure might have a dual function, one normatively problematic and the other not. Laws criminalizing use of a secret compartment in a car are illustrative. Such a compartment might be used to conceal contraband, such as illegal drugs, but it might also be used to better conceal from view valuable lawful items (such as expensive camera equipment).⁹²

The dual-use concern was addressed by the Illinois Supreme Court in a decision invalidating on due process grounds its state law making it a felony “for any person to own or operate any motor vehicle he or she knows to contain a false or secret compartment.”⁹³ The Court reversed the convictions of three individuals, none of whom had contraband stored in their compartments, finding that the law, which lacked proof of any criminal purpose, did not constitute a “reasonable means of preventing the targeted conduct”:

The statute potentially criminalizes innocent conduct, as it visits the status of a felon upon anyone who owns or operates a vehicle he or she knows to contain a false or secret compartment, defined as one intended and designed to conceal the compartment or its contents from law enforcement officers. The contents of the compartment do not have to be illegal for a conviction to result.⁹⁴

The Court rejected “the notion that the intent to conceal something from law enforcement officers necessarily entails illegal conduct...Just as citizens are not required to display their worldly possessions to the general public, neither are they required to exhibit them for the plain view of law enforcement.”⁹⁵

Footnote 91 (continued)

getting off with a warning instead of a ticket are slim to none, as officers usually count the radar detector as warning enough”).

⁹² Presumably in response to this demand, several cars come with factory-equipped hidden compartments. Peter Jones, “6 Cars with Hidden Compartments (With Pictures)”, *Motor and Wheels.Com* (Jan. 18, 2021), <https://motorandwheels.com/popular-cars-with-hidden-compartments/>.

⁹³ *People v. Carpenter*, 888 N.E.2d 105, 109 (Ill. 2008) (citation omitted).

⁹⁴ *Ibid.*, p. 117.

⁹⁵ *Ibid.* A more risqué example of such dual use is found in the marketing of the false prosthetic penis Whizzinator, which can be used to avoid providing a “dirty” urine, but also, according to its manufacturer, for “pranks and [sexual] pleasure.” <https://whizzinator.com/what-to-look-for-when-buying-a-synthetic-urine-kit/>.

Dual-use items can also have broader societal benefit.⁹⁶ Allowing them, especially with non-serious offenses, can provide a beneficial sphere of personal autonomy, permitting a degree of “slack” in the daily lives of individuals.⁹⁷ They can afford a perhaps welcome “sporting chance of getting away with crime, especially the ordinary everyday offenses that all of us might commit.”⁹⁸ They can also provide a measure of relief from discriminatory police practices. A large literature demonstrates the tendency of law enforcement to single out minority motorists⁹⁹ and pedestrians,¹⁰⁰ with at times fatal results,¹⁰¹ for low-level offenses, including on the basis of a pretextual motivation.¹⁰²

Detection avoidance measures can also mitigate the negative impact of modern surveillance technologies. Automated tools employed by police such as networked surveillance cameras, license plate readers, and facial recognition technology provoke concern because they are cheap and easy to use, and the data they generate can be stored indefinitely and fused with other information.¹⁰³ In combined effect, the technologies achieve what the Supreme Court has called a “near perfect surveillance,” not only of criminal suspects, but “everyone.”¹⁰⁴ Exacerbating matters, as

⁹⁶ Radar detectors used by motorists, lawful in the vast majority of U.S. jurisdictions, are illustrative. Motorists can rely on the signal emitted by a radar detector to decrease their speed when police are present, and drive within the speed limit thereafter, using the device as a warning mechanism, with a social benefit (safer roadways) resulting. However, many, indeed likely most motorists, only decrease their speed temporarily, resuming their unlawful speed when police are not in the vicinity. In the latter scenario, a radar detector enables law-breaking.

⁹⁷ See generally Shu-Yi Oei & Diane M. Ring, “‘Slack’ in the Data Age”, *Alabama Law Review* 73(1) (2021): pp. 47–106, p. 50.

⁹⁸ Ronald V. Clarke, “Situational Crime Prevention”, *Crime & Justice* 19 (1995): pp. 91–150, p. 135. See also Edward K. Cheng, “Structural Laws and the Puzzle of Regulating Behavior”, *Northwestern Law Review* 100(2) (2006): pp. 655–717, p. 671 (recognizing an autonomous need for “freedom to break the law” and the “liberty interest in voluntary compliance”).

⁹⁹ Frank R. Baumgartner et al., *Suspect Citizens: What 20 Million Traffic Stops Tell Us About Policing and Race* (Cambridge: Cambridge University Press, 2018); David A. Harris, “Racial Profiling: Past, Present, and Future?”, *Criminal Justice* 34 (2020): pp. 10–22.

¹⁰⁰ Elise C. Boddie, “Racially Territorial Policing in Black Neighborhoods”, *University of Chicago Law Review* 89(2) (2022): pp. 477–98.

¹⁰¹ Devon W. Carbado, “From Stopping Black People to Killing Black People: The Fourth Amendment Pathways to Police Violence”, *California Law Review* 105(1) (2017): pp. 125–64.

¹⁰² See *Whren v. United States*, 517 U.S. 806 (1996) (holding that pretextual motivation for an auto stop was constitutionally reasonable so long as police had probable cause to conclude that a driving offense of some kind was committed). Research has also shown that police target poor and minority community members to generate funds from fines and fees, which detection avoidance measures can also protect against. See Wayne A. Logan, “What the Feds Can Do to Rein in Local Mercenary Criminal Justice”, *Illinois Law Review* 2018(5) (2018): pp. 1731–59; Kaveh Waddell, “How License-Plate Readers Have Helped Police and Lenders Target the Poor”, *Atlantic* (Apr. 22, 2016).

¹⁰³ See Christopher Slobogin, “Panvasive Surveillance, Political Process Theory, and the Non-Delegation Doctrine”, *Georgetown Law Journal* 102(6) (2014): pp. 1721–76 (coining the phrase “panvasive state,” where surveillance is both “pervasive and invasive”). Moreover, the Fourth Amendment frequently provides no protection against the warrantless use of modern surveillance technologies by law enforcement. See Gregory Brazeal, “Mass Seizure and Mass Search”, *University of Pennsylvania Journal of Constitutional Law* 22(4) (2020): pp. 1001–72, p. 1003 (noting that “the Fourth Amendment...currently provides no protection against the vast majority of existing and possible forms of digital mass surveillance”).

¹⁰⁴ *Carpenter v. United States*, 138 S. Ct. 2206, 2212, 221 (2018).

with enforcement more generally, police surveillance efforts often target poor and minority communities,¹⁰⁵ which can mistakenly result in false positives,¹⁰⁶ and otherwise sweep up law-abiding citizens who simply wish to avoid contact with “the system.”¹⁰⁷ Surveillance, moreover, is not only undertaken by police. Businesses and community members employ millions of surveillance devices, such as the Amazon Ring doorbell camera,¹⁰⁸ recording legal and illegal activity alike,¹⁰⁹ which can have a chilling effect on personal liberty.¹¹⁰

Finally, relatedly, detection avoidance measures can help protect the exercise of First Amendment-protected activity. Recent media reports highlight how law enforcement, at times in tandem with private data aggregators, secretly surveilled and identified participants in Black Lives Matter protests.¹¹¹ Detection avoidance in such circumstances can constitute “privacy protests,” “actions individuals take to block or to thwart surveillance for reasons unrelated to criminal wrongdoing.”¹¹² The website of the Veil license plate coating material, noted earlier, echoes this view, declaring that it protects users from police surveillance, especially automated license plate reading (ALPR) technology,¹¹³ “systems that are touted as enhancing

¹⁰⁵ Simone Brown, *Dark Matters: On Surveillance of Blackness* (Durham: Duke University Press, 2015); Barton Gellman & Sam Adler-Bell, Century Foundation, *The Disparate Impact of Surveillance* (Dec. 21, 2017).

¹⁰⁶ See, e.g., Kashmir Hill, “Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match”, *N.Y. Times* (Dec. 29, 2020), p. B1. Facial recognition inaccuracies are especially likely with non-white individuals. Tom Simonite, “The Best Algorithms Struggle to Recognize Black Faces Equally”, *Wired* (July 22, 2019), <https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/>.

¹⁰⁷ Sarah Brayne, “Surveillance and System Avoidance: Criminal Justice Contact and Institutional Attachment”, *American Sociological Review* 79(3) (2014): pp. 367–91; Jamie J. Fader, “Managing Risk and Uncertainty Through Network Avoidance”, *Criminology* 59(1) (2021): pp. 1–26.

¹⁰⁸ Evan Greer, “America’s Ring Doorbell Camera Obsession Highlights the Scourge of Mass Surveillance”, NBC.com (Nov. 1, 2022), <https://www.nbcnews.com/think/opinion/amazons-ring-doorbell-vid-eos-make-america-less-safe-crime-rcna55143>.

¹⁰⁹ See, e.g., Sanil Chinoy, “The Racist History Behind Facial Recognition”, *N.Y. Times* (July 10, 2019), p. 3 (noting that facial recognition technology can identify the emotional states of surveilled individuals).

¹¹⁰ See generally Neil M. Richards, “The Dangers of Surveillance”, *Harvard Law Review* 126 (2013): pp. 1934–65.

¹¹¹ Katelyn Ringrose & Divya Ramjee, “Watch Where You Walk: Law Enforcement Surveillance and Protester Privacy”, *California Law Review Online* 11 (2020): pp. 349–66.

¹¹² Elizabeth E. Joh, “Privacy Protests: Surveillance Evasion and Fourth Amendment Suspicion”, *Arizona Law Review* 55 (2013): pp. 997–1029, pp. 1000–01; see also *ibid.*, p. 998 (“Privacy protests often appear no different from criminal evasiveness, but they merit recognition as important sources of resistance to the increasing capabilities of government surveillance.”).

¹¹³ See generally Christopher S. Koper & Cynthia Lum, “The Impacts of Large-Scale License Plate Reader Deployments on Criminal Investigations”, *Police Quarterly* 22(1) (2019): pp. 305–29, pp. 309, 321. The automated readers “suck in the license plates of motorists around them, geolocating where those cars are at that moment. Originally the point of ALPRs was to compare the reads to a ‘hot list,’ such as to detect stolen vehicles...[Today, an ALPR] turns ordinary police car dash cams into powerful tools that can collect reads from traffic across three lanes, front and back, as police cars move on patrol.” Barry Friedman, “Private Data/Public Regulation”, Hoover Institution, Aegis Series Paper No. 2105 (Oct. 4, 2022), 4 (footnotes omitted).

public safety,” yet are “exact[ing] [a price] on our individual liberties [that] is exceedingly high....”¹¹⁴

4 Implementation

Presuming detection avoidance warrants criminalization, in some instances, what to do? Two primary legal options come to mind.¹¹⁵

One option is to criminalize detection avoidance measures themselves, *simpliciter*, regardless of the nature or seriousness of the underlying offenses actors seek to avoid accountability for committing. Stand-alone criminalization of a silencer, for instance, is thought justified because there are few lawful uses for a silencer.¹¹⁶

Such an approach, however, must be sensitive to over-inclusiveness concerns, especially when dual-use measures are involved (discussed above).¹¹⁷ In such instances, criminal liability should be conditioned upon an actor’s *mens rea*. Much as how determining whether an object qualifies as a “deadly weapon” focuses not on the nature of an item, but rather the actor’s purpose in using it,¹¹⁸ the criminalization of detection avoidance should depend on the intent of the party.¹¹⁹ For example, a law might specify intent to evade, such as with tools to thwart anti-shoplifting security.¹²⁰ Another example is found in Ohio’s law concerning car secret compartments,

¹¹⁴ Laser Veil Stealth Coatings FAQs, <https://www.stealthveil.com/faq/>. The company’s website warns that police use ALPR to “amass[] huge amounts of information relating to travel patterns and places of gathering (including gun shows and political rallies) of countless law-abiding citizens. This is tantamount to living in one globalized hidden police-state.” <https://veilstealth.com/pages/how-laser-veil-g6-stealth-coating-protects-you>. Elsewhere, Veil assures prospective purchasers that “[f]ortunately[,] the countermeasure industry and those concerned about taking back our privacy rights has [sic] devised several solutions to this growing threat to our civil liberties.” “Protecting Your Privacy from ALPR/ANPR Automatic License Plate Recognition Systems”, <https://veilstealth.com/blogs/news>.

¹¹⁵ In some limited circumstances, a soft, non-legal approach might be undertaken. For instance, faced with a rash of thefts, several years ago stores in Los Angeles required that customers remove their hats and pull their sweatshirt hoods off their heads before entering, a practice dating back to King Carlos III of Spain in the 1700s, who banned the wearing of broad hats to curb robberies and other crimes. Richard Winton, “New LAPD Crime-Busting Strategy: Hats Off Before Entering Stores”, *L.A. Times* (Oct. 12, 2011), <https://www.latimes.com/social/glendale-news-press/news/tn-gnp-xpm-2011-10-12-tn-818-1012-crime-story.html>. For a more recent instance see Megan Cerullo, “New York Police Say Shoppers Should Take Off Their Masks Before Entering Stores”, CBS News, CBSNews.com (March 1, 2023), <https://www.cbsnews.com/news/face-masks-robbery-nypd-require-customers-remove-covid-19/>.

¹¹⁶ See *United States v. Hall*, 171 F.3d 1133, 1155 (8th Cir. 1999) (Panner, J., concurring) (noting that “[i]t is difficult to conceive of any legitimate purpose for which a private citizen needs a silencer.”).

¹¹⁷ For discussion of mask bans, created to combat the Ku Klux Klan, and how they today are being used to target political protesters see Rob Kahn, “The Long Road Back to Skokie: Returning the First Amendment to Mask Wearers”, *Journal of Law & Policy* 28 (2020): pp. 71–149, p. 74.

¹¹⁸ Chad Flanders & Desiree Austin-Holliday, “‘Dangerous Instruments’: A Case Study in Over-Criminalization”, *Missouri Law Review* 83(2) (2018): pp. 259–99.

¹¹⁹ As Sandra Mason has observed, “[a] single hammer can have many purposes. The purpose of any particular hammer depends on its context and the intention of the person who wields it.” Sandra G. Mason, “The Concept of Criminal Law”, *Criminal Law and Philosophy* 14(3) (2020): pp. 447–64, p. 457.

¹²⁰ See, e.g., N.Y. Penal Law s. 170.47 (2021) (requiring intent to thwart antishoplifting device by use of an anti-security item).

which makes it a crime to “knowingly operate, possess, or use a vehicle with a hidden compartment with knowledge that the hidden compartment is used or intended to be used to facilitate the unlawful concealment or transportation of a controlled substance.”¹²¹

Intent, of course, is a cornerstone of criminal liability.¹²² Under the classic formulation of the *Model Penal Code*, an individual acts with criminal “purpose” if it is “his conscious object to engage in conduct of that nature or to cause such a result”¹²³; acts “knowingly” if he is aware that his conduct is of that nature or that such circumstances exist¹²⁴; and acts “recklessly” if he “consciously disregards a substantial and unjustifiable risk that the material element exists or will result from his conduct.”¹²⁵

While one of the aforementioned mental states, or a reformulation of it,¹²⁶ is essential, proof will often be difficult to secure, and will vary from case to case. In many instances, however, line-drawing will not be difficult. Most obvious is the situation where the party is in fact detected engaging in unlawful activity, and their avoidance effort is foiled—for instance, when the possessor of child pornography is found to have used a form of encryption that police somehow were able to circumvent or defeat.¹²⁷ Or when an individual utilizes a privacy-protecting measure when not engaging in unlawful activity, such as when attending a lawful political protest.

Imposition of a mens rea requirement will have the corollary benefit of reducing the likelihood that criminalized avoidance measures will be treated as “proxy crimes,” which “while not inherently risking harm[s], stand[] in for behavior that does risk harm.”¹²⁸ As Youngjae Lee recently noted, proxy crime laws are problematic because they “are *designed* to sweep both morally innocent and morally

¹²¹ Ohio Stat. s. 2923.241(C) (2020). Burglar tools afford another example. See, e.g., N.Y. Penal Law s. 140.35 (2021) (requiring intent to use or knowledge that another intends to use item in certain property crimes); *People v. Borrero*, 259 N.E.2d 902, 905 (N.Y. 1970) (noting that while screwdrivers are not burglar tools per se, the accompanying circumstances can establish intended use in burglary).

¹²² See Douglas Husak, “The Costs to Criminal Theory of Supposing that Intentions are Irrelevant to Permissibility”, *Criminal Law and Philosophy* 3(1) (2009): pp. 51–70, p. 58 (recognizing that “intentions are partly constitutive of the criminal act itself”). See also generally Francis X. Shen et al., “Sorting Guilty Minds”, *New York University Law Review* 86(5) (2011): pp. 1306–60.

¹²³ *Model Penal Code* s. 2.02(2)(a)(i).

¹²⁴ *Ibid.* s. 2.02(2)(b)(i).

¹²⁵ *Ibid.* s. 2.02(2)(c).

¹²⁶ Although mental states can be hard to discern and distinguish, recent research appears to be making inroads, for instance showing among test subjects an apparent brain-based distinction between knowing and reckless mental states. Owen D. Jones, Read Montague, & Gideon Yaffe, “Detecting Mens Rea in the Brain”, *University of Pennsylvania Law Review* 169(1) (2020): pp. 1–31.

¹²⁷ In some instances, circumstantial evidence of intent to avoid a criminal prohibition will be available. See, e.g., *United States v. Ramos-Rodriguez*, 809 F.3d 817, 822–23 (8th Cir. 2016) (noting decisions where circumstantial evidence of guilty knowledge is thought needed when drugs are found hidden in a car’s secret compartment).

¹²⁸ Richard H. McAdams, “The Political Economy of Entrapment”, *Journal of Criminal Law & Criminology* 96(1) (2005): pp. 107–85, pp. 159–60. See also Brenner Fissell, “Abstract Risk and the Politics of the Criminal Law”, *American Criminal Law Review* 51 (2014): pp. 657–87 (discussing “abstract endangerment” laws, such as those criminalizing underage possession of alcohol, which punish not the actual, but hypothetical, creation of risk).

wrongful together into one class.”¹²⁹ Requiring that the government prove intent to evade detection for an underlying offense will significantly reduce the threat that detection avoidance will serve a proxy function, a threat that can be further reduced by use of prosecutorial charging guidelines.¹³⁰

A second option is to enhance the punishment of the underlying offense, when detected despite use of a detection avoidance measure. Ohio’s secret car compartment law takes this approach: using a compartment to hide contraband is punished more severely than possession of the contraband alone.¹³¹ A similar approach is taken in the punishment of financial crimes under the U.S. Sentencing Guidelines whereby an individual’s sentence is increased if the wrongdoing “involved sophisticated means and the defendant intentionally engaged in or caused the conduct constituting sophisticated means.”¹³² In such a situation, the punishment attaching to use of the avoidance measure might be increased independently of the seriousness of the underlying offense, or it might be correlated with it.

5 Conclusion

This article began with a question: are detection avoidance measures “courageous and inspiring expressions of the human spirit,” or do they qualify as “destructive antisocial behavior” worthy of criminal condemnation? As the preceding discussion suggests, the question does not admit of a categorical response. Nevertheless, it is hoped that the article has imposed a helpful degree of analytic order upon the broad array of detection avoidance measures individuals now employ, and will employ in the future, and that discussion of their ramifications inspires additional inquiry into the overlooked yet important and pervasive phenomenon.

Acknowledgements The author thanks Joshua Dressler, Antony Duff, Stuart Green, Douglas Husak, David Logan, Sandra Mason, Sarah Swan, Manuel Utset, and Eugene Volokh for their very helpful comments on the piece.

¹²⁹ Youngjae Lee, “Proxy Crimes and Overcriminalization”, *Criminal Law and Philosophy* 16 (2022): pp. 469–84, pp. 473–74. Proxy crimes are also thought problematic because they effectively lower the state’s constitutional duty of proving beyond a reasonable doubt the elements of the correlated more serious offense. McAdams, “The Political Economy of Entrapment”, p. 162.

¹³⁰ See generally John E. Pfaff, “Prosecutorial Guidelines”, in Erik Luna (ed.), *3 Reforming Criminal Justice: Pretrial and Trial Processes* (Phoenix, Az.: Arizona State University, 2017), pp. 101–20.

¹³¹ See Ohio Stat. s. 2923.241(F) (2021) (operating a vehicle with a hidden compartment used to transport a controlled substance is a second-degree felony, whereas having a secret compartment without drugs inside is a third-degree felony).

¹³² *U.S. Sentencing Guidelines* s. 2B1.1(b)(10)(A),(C). See also *U.S. Sentencing Guidelines Manual* app. C, amend. 577 (2003) (stating that Commission increased sentences “for fraud offenses that involve conduct...that makes it difficult for law enforcement authorities to discover the offense or apprehend the offender”). Cf. Vimal Patel, “Man Who Threatened to Kill Fauci Is Sentenced to 3 Years in Prison”, *N.Y. Times* (Aug. 4, 2022), <https://www.nytimes.com/2022/08/04/us/fauci-thomas-connally-sentenced.html> (quoting prosecutors who noted at sentencing that the “[s]mart and technologically sophisticated” defendant used a “foreign encrypted email” to send threats to government officials, in order to “heighten the terror” and obscure his identity).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.