CHARTING THE SKIES: WHERE DOES FACIAL RECOGNITION TECHNOLOGY "FIT" IN THE DATA PRIVACY COSMOS?

Steven D. Zansberg

CHARTING THE STARS: WHERE DOES FACIAL RECOGNITION TECHNOLOGY "FIT" IN THE DATA PRIVACY COSMOS?

Steven D. Zansberg

INTRODUCTION

Last Fall, I was invited to speak at an annual law school symposium about the potential risk to personal privacy posed by Facial Recognition Technology ("FRT").[1] The ever-expanding use of FRT, by law enforcement for investigating and prosecuting crimes and by a multitude of private companies for a wide variety of commercial applications, has been very much in the news of late.[2] Multiple lawsuits are presently pending across the nation, and the globe, that call upon judges and juries to resolve a clash of rights.[3] On the one hand, people have the right to use information that was freely exposed on public streets and on the internet; on the other hand, the subjects of photographic images, which provide access to a wide array of other personal information about themselves, have the right to personal autonomy–to be let alone. In late June 2020, Massachusetts Senator Edward Markey, joined by four other Senators, introduced a bill that would prohibit federal and state law enforcement

---

[1] *See* Session Recording: The Privacy Foundation at the University of Denver Sturm College of Law, *Facial Recognition & Privacy* (Oct. 30, 2020), https://www.law.du.edu/privacy-foundation. This essay presumes a basic understanding of how FRT works and some familiarity with its real-world applications. For a concise introduction to both, see Lucas Scott, *What Is Facial Recognition? - Applications & How it Works*, LIONBRIDGE (Oct. 25, 2019), https://lionbridge.ai/articles/what-is-facial-recognition/; *see also* GOV'T ACCOUNTABILITY OFFICE, FACIAL RECOGNITION TECHNOLOGY (July 2020), https://www.gao.gov/assets/710/708045.pdf; CONG. RES. SERV., FEDERAL LAW ENFORCEMENT USE OF FACIAL RECOGNITION TECHNOLOGY (Oct. 27, 2020), https://crsreports.congress.gov/product/pdf/R/R46586.

[2] *See, e.g.*, *Rights Groups Call for Ban of 'Invasive' Face Recognition Tech*, ALJAZEERA (June 3, 2021), https://www.aljazeera.com/news/2021/6/3/rights-groups-call-for-ban-of-invasive-face-recognition-tech.; Elissy Salamy, *Your Photo Could Already Be in a Facial Recognition Database*, WJLA (June 7, 2021), https://wjla.com/news/nation-world/your-photo-could-already-be-in-a-facial-recognition-database; Kylie McGivern, *Facial Recognition Meant to Stop Unemployment Fraud is Blocking Legitimate Applicants*, ABC ACTION NEWS (June 7, 2021, 6:27 AM), https://www.abcactionnews.com/news/local-news/i-team-investigates/facial-recognition-meant-to-stop-unemployment-fraud-is-blocking-legitimate-applicants. *See also* Matthew Feeney, *Facial Recognition Technology Is Getting Out of Control,* BUS. INSIDER (Mar. 8, 2020), https://www.businessinsider.com/facial-recognition-technology-getting-out-of-control-needs-regulation-2020-3.

[3] *See, e.g.* J.D. Tuccille, *Lawsuit Challenges Clearview's Use of Scraped Social Media Images for Facial Recognition*, REASON (Mar. 15, 2021), https://reason.com/2021/03/15/lawsuit-challenges-clearview-use-of-scraped-social-media-images-for-facial-recognition/; Tate Ryan-Mosley, *The New Lawsuit That Shows Facial Recognition Is Officially A Civil Rights Issue*, MIT TECH. REV. (Apr. 14, 2021), https://www.technologyreview.com/2021/04/14/1022676/robert-williams-facial-recognition-lawsuit-aclu-detroit-police/; Amanda Bronstad, *NY-Based Facial Recognition Tech Company Wrangles With Judges in Two States Over Privacy Class Actions,* N.Y.L.J., (Sept.10, 2020), https://www.law.com/newyorklawjournal/2020/09/10/ny-based-facial-recognition-tech-company-wrangles-with-judges-in-two-states-over-privacy-class-actions/.

agencies from using FRT until further federal legislation authorizes its use.[4] In June of 2021, King County, Washington became the first in the nation to ban the use of FRT by all government agencies.[5] Several cities and states have limited the use of FRT to investigate crimes, or barred it outright.[6]

Although the symposium organizer, Professor John Soma, had instructed all panelists to "come as you are," I disobeyed and boned up on the current state of the law. The challenge that stood out was striking a balance between the First Amendment rights of publishers and other providers, i.e., the Clearview AIs of the world, and the right of individuals "to be let alone." Information providers have a right to collect information that others have intentionally left open to public view and may analyze and distribute that data.[7] On the other hand, individuals should be free to browse the internet without fear that their photographs and information will be used without their consent by commercial marketers, insurance companies, airlines, or government prosecutors, for whatever purposes they desire. The data points available through our online activity, whether publicly available or not, can be combined with other data points to assemble a mosaic of life experience, including, potentially, our most intimate "secrets."[8]

---

[4] *See* The Facial Recognition and Biometric Technology Moratorium Act of 2020, S. 4084, 116th Cong. (2020), https://www.congress.gov/bill/116th-congress/senate-bill/4084. *See also* Press Release from Ed Markey, Senator, United States Senate, Senators Markey and Merkley, and Reps. Jayapal, Pressley to Introduce Legislation to Ban Government Use of Facial Recognition, Other Biometric Technology (June 25, 2020), https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal-pressley-to-introduce-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology.

[5] Aya Elamroussi, *This Washington County Is the First to Ban Facial Recognition Technology, Official Says*, CNN (June 2, 2021, 8:43 AM), https://www.cnn.com/2021/06/02/us/facial-recognition-technology-ban/index.html.

[6] *See* Laura Hautala, *San Francisco Becomes First City to Bar Police From Using Facial Recognition*, CNET (May 14, 2019, 4:06 PM), https://www.cnet.com/news/san-francisco-becomes-first-city-to-bar-police-from-using-facial-recognition/; Jason Plautz, *Boston Is Second-Larges US City to Ban Facial Recognition*, SMART CITIES DIVE (July 6, 2020), https://www.smartcitiesdive.com/news/boston-is-second-largest-us-city-to-ban-facial-recognition/581008/; Jeff Adelson, *New Orleans to Reform Police Use of Facial Recognition Tech*, GOV. TECH. (Dec. 21, 2020), https://www.govtech.com/public-safety/new-orleans-to-reform-police-use-of-facial-recognition-tech.html; Kashmir Hill, *New Jersey Bars Police From Using Clearview Facial Recognition App*, N.Y. TIMES (Jan. 24, 2020), https://www.nytimes.com/2020/01/24/technology/clearview-ai-new-jersey.html; Tommy Wiita, *Minneapolis City Council Votes to Bar Use of Facial Recognition Technology*, EYEWITNESS NEWS (Feb. 12, 2021, 12:21 PM), https://kstp.com/minnesota-news/minneapolis-city-council-votes-to-bar-use-of-facial-recognition-technology-with-narrow-exceptions/6010852/.

[7] *See* Chris Morran, *House Votes to Allow Internet Service Providers to Sell, Share Your Personal Information*, CONSUMER REPORTS (Mar. 28, 2017), https://www.consumerreports.org/consumerist/house-votes-to-allow-internet-service-providers-to-sell-share-your-personal-information/; Mike Snider, *ISPs Can Now Collect and Sell Your Data: What to Know About Internet Privacy Rules*, USA TODAY (Apr. 4, 2017, 10:14 PM), https://www.usatoday.com/story/tech/news/2017/04/04/isps-can-now-collect-and-sell-your-data-what-know-internet-privacy/100015356/.

[8] *See, e.g.*, Gabriel R. Schlabach, Note, *Privacy in The Cloud: The Mosaic Theory and The Stored Communications Act*, 67 STAN. L. REV. 667, (2017); Lance Selva, William Shulman & Robert Rumsey, *Rise of the Mosaic Theory: Implications for Cell Site Location Tracking by Law Enforcement,* 32 J. MARSHALL J. INFO. TECH. & PRIV. L. 235, (2016). We are all aware of the existing use, by multiple parties, of correlations

What I offer below is a theoretical framework for evaluating competing societal interests: the value our society assigns to the free-flow of information to the public, including highly sophisticated computer-generated analyses of gargantuan data sets–information that helps inform better individual and collective decision-making; and on the other hand, the value we place on privacy even in the context of technological advances. One's most personal actions and thoughts–what we type into search engines, which videos we watch, for how long or how often, which books or articles we read, with whom we communicate and the contents of those communications–should not be rendered public information merely by our using Facebook, Google, Amazon, Instagram, YouTube, Hulu, WhatsApp, or Zoom, or because our faces are posted on the internet, with or without consent.

This essay posits a schematic matrix defined by three interrelated indices by which, I believe, any new and potentially privacy-intruding technology may be assessed. I then proceed to identify and "plot" onto that rubric a handful of judicial precedents which serve as recognized guideposts, collectively forming the "constellation" into which any new "star" may be appropriately mapped.

I. THE FRAMEWORK

A. Privacy . . . From Whom?

Any discussion of the *right* of privacy must begin with a quick overview of the *law* of privacy, to the extent that there is such a thing. There is a broad array of so-called privacy rights, including the right to exercise personal autonomy,[9] to make decisions concerning one's own body and mind,[10] and which behaviors in which to engage in the solitude of one's own home.[11] The particular right of privacy that is the focus of this essay has been referred to as "the right to be let alone"[12] from uninvited prying into, and exposure of, one's dignity, persona, and other related personal demographic information. Of course, there are two categories of actors who can intrude on, and thereby violate, that zone of

---

between people who have purchased certain products and services and their voting patterns and party affiliation. *See, e.g.*, Maddy Martin, *Politics and Personal Driving Preferences: Do Republicans and Democrats Drive Different Cars?,* MAD MECHANIC (Feb. 12, 2016), https://www.yourmechanic.com/article/red-car-blue-car-do-political-views-predict-car-preferences. *See also* Erin Delmore, *Whole Foods? Cracker Barrel? What You Eat Tells How You Vote*, MSNBC (Nov. 14, 2012), https://www.msnbc.com/the-cycle/whole-foods-cracker-barrel-msna15970.

[9] "Personal autonomy" is used to encompass a great number of personal freedoms that fall under the privacy rights umbrella. *See e.g.*, NAACP v. Alabama, 357 U.S. 449 (1958) (protecting the freedom of association); Shapiro v. Thompson, 394 U.S. 618 (1969) (establishing a right to travel); Meyer v. Nebraska, 262 U.S. 390 (1923) (protecting the right to teach and learn foreign languages); Pierce v. Soc'y of Sisters, 268 U.S. 510 (1925) (preventing states from compelling students to attend public schools). *See also Privacy Rights and Personal Autonomy*, JUSTIA, https://bit.ly/2TSaKX3 (last updated Apr. 2018).

[10] *See e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965) (the right of marital privacy); Roe v. Wade, 410 U.S. 113 (1973) (access to abortion).

[11] *See e.g.*, Stanley v. Georgia, 394 U.S. 557 (1969) (holding that use of pornography is part of the personal autonomy right).

[12] *See generally* Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

personal privacy who are treated differently under the law: governmental actors and non-governmental actors.[13]

Notwithstanding the fact that the same affront or injury to one's expectation of privacy may be experienced regardless of whether the transgressor is imbued with governmental authority, the protections *the law* provides us turn in large part on *who* committed the violation.[14] The United States Constitution acts as a check and balance on the actions only of government actors "acting under the color of" state or federal law.[15] Simply put, the Constitution has no application, whatsoever, to purely private actors.[16] Thus, only the FBI, local police, public school authorities, and other similar agencies and their individual employees, vested with governmental authority, can violate one's *constitutional* right to privacy; not so for the Facebooks, Instagrams, or Clearview AIs of the world.[17] So, we will first discuss the constitutional limitations on governmental actors' actions before moving to limitations that statutes and judge-made law have imposed on *non*-governmental, private actors' actions.

B. The Constitutional Right of Privacy

"In which provision(s) of the U.S. Constitution do either the word 'privacy' or 'private' appear?" This is a well-worn "trick" law school question, because the correct answer is *none*. Neither word appears anywhere in the Constitution of the United States or in the Declaration of Independence. Nevertheless, there are two bodies of constitutional restrictions on governmental actors: the Fourth Amendment,[18] and the more general "right of privacy" the Justices have found arises from the interplay of various other constitutional provisions (as well as their interstices).[19]

i. Unreasonable searches and seizures. The Fourth Amendment protects everyone in the country from "unreasonable search or seizure" of our bodies, personal effects, papers, or other possessions.[20] Thus, in order to gain entry into your home without your consent, or to search your handbag, office, or car, a law enforcement officer must obtain a

---

[13] *See generally* Sam Kamin, *The Private is Public: The Relevance of Private Actors in Defining the Fourth Amendment*, 46 B.C. L. REV. 83 (2004).

[14] *Id.* at 85 n. 9.

[15] For additional discussion of the state action doctrine, see Martha Minow, *Alternatives to the State Action Doctrine in the Era of Privatization, Mandatory Arbitration, and the Internet: Directing Law to Serve Human Needs*, 52 HARV. CIV. RIGHTS-CIV. LIBERTIES L. REV. 145 (2006).

[16] Jarod Bona, *The State Action Doctrine for Federal Constitutional Claims*, IR GLOBAL (Aug. 26, 2020), https://www.irglobal.com/article/the-state-action-doctrine-for-federal-constitutional-claims/.

[17] *See e.g.*, Elizabeth Smith & Johanna Zelman, *The First Amendment: Where it Is Implicated, and Where it Is Not*, JDSUPRA (Jan. 12, 2021), https://www.jdsupra.com/legalnews/the-first-amendment-where-it-is-3482126/. There is also a hefty body of case law denying Section 1983 claims against big tech companies because they are not governmental entities. *See e.g.*, Abid v. Google, LLC, No. 18-cv-00981-MEJ, 2018 WL 1784085, at *3 (N.D. Cal. Apr. 13, 2018); Fed. Agency of News LLC v. Facebook, Inc., 395 F. Supp. 3d 1295, 1304 (N.D. Cal. 2019).

[18] U.S. CONST. amend. IV.

[19] *See* Griswold v. Connecticut, 381 U.S. 479 (1965).

[20] U.S. CONST. amend. IV.

warrant authorizing such a search, issued and signed by a judge.[21] This is only possible upon a finding of sufficient facts alleged under oath which establish "probable cause" to believe a crime has been committed, and that there is evidence in the object of search that is potentially relevant to the crime.[22] Only the presence of exceptional "exigent circumstances" are enough to waive this requirement.[23]

ii. The General Constitutional "Right of Privacy." Beyond the Fourth Amendment's "search and seizure" provision, the Supreme Court has recognized that there is a more generalized "right to be let alone" by government agents. This right, though not explicitly set forth in the Constitution's text, is found in the penumbras of several textual provisions.[24] The parameters of this common-law right of personal privacy is discussed in greater detail below.

C. Non-Governmental Violators of Personal Privacy

Intrusions such as unauthorized discovery or disclosure of highly personal facts are no less offensive to the victim if the intruder or privacy violator is a purely private actor, not enshrouded with governmental authority. While the U.S. Constitution has no application to such actors, civil and criminal state law places limits on such incursions. A host of state and federal statutes impose criminal or civil penalties for a private party's interception or use of telephonic communications without consent (i.e., wiretapping), or for disclosing personal identifying information (including medical records, video rental records, or social security numbers) without consent, among other prohibited acts.[25] Because a subset of these statutes impose government-mandated penalties on the exercise of speech and expression, the First Amendment places limits on such statutes, as will be discussed below.

---

[21] *See e.g.*, Collins v. Virginia, 138 S. Ct. 1663 (2018).

[22] *See* Missouri v. McNeely, 569 U.S. 141, 149 (2013) (giving examples of exigencies sufficient to justify a warrantless search, such as "law enforcement's need to provide emergency assistance to an occupant of a home . . . engage in 'hot pursuit' of a fleeing suspect . . . or enter a burning building to put out a fire and investigate its cause.") Police may search a car without a warrant if there is probable cause to believe evidence of a crime is inside the car. *See* Carroll v. United States, 267 U.S. 132 (1925). However, they may not search a covered vehicle on a private property without a warrant. *Collins*, 138 S. Ct. at 1675.

[23] *McNeely*, 569 U.S. at 149.

[24] *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 484–85 (1965) ("specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees [in the Bill of Rights] create zones of privacy . . . . We have had many controversies over these penumbral rights of "privacy and repose." These cases bear witness that the right of privacy which presses for recognition here is a legitimate one."); Roe v. Wade, 410 U.S. 113, 152 (1973) ("[t]he Constitution does not explicitly mention any right of privacy. In a line of decisions, however . . . the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution."); *Id.* at 129, (recognizing one asserted basis for a woman's "right" to terminate a pregnancy, "in personal, marital, familial, and sexual privacy said to be protected by the Bill of Rights or its penumbras . . . .").

[25] *See e.g.*, 18 U.S.C. § 2511 (prohibiting wiretapping); Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (medical records are protected from unauthorized private access under the Act); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (requiring video stores to destroy rental records no longer than one year after a customer account is terminated).

In addition to the ever-expanding morass of statutes that protect personal privacy, the common law recognizes two civil tort claims for invasion of privacy arising from the unauthorized access to, or disclosure of, truthful[26] personal and private information: (1) intrusion upon seclusion,[27] and (2) publicity given to private facts.[28] The former provides for a right of action against one or more people who have intruded, without the plaintiff's consent, into a sphere of personal privacy, whether through physical presence (e.g., entering a hospital room or bedroom),[29] or through unauthorized access to highly personal and private information (e.g., one's mental health treatment records, or HIV test results).[30] The latter claim arises from the unauthorized public disclosure of truthful information about another that was previously "private" (not previously disclosed) and highly personal–such that unconsented-to disclosure would be "highly offensive" to a reasonable person.[31] Both of these civil torts turn on whether the physical or virtual "space" intruded upon, or the information publicly disclosed without the individual's consent, is of a sufficiently "highly personal and private" nature in the mind of a hypothetical *objective* victim, to give rise to a "reasonable expectation of privacy."[32] For example, it is generally accepted that a person's medical and mental health records are of a sufficiently private, personal, or sensitive nature that a health care provider may not reveal such information to the public without the patient's authorization.[33] Such a disclosure is prohibited by federal law.[34] In contrast, matters of public record, or information that has been "freely left open" to the public at large by the subject of that information cannot give rise to a legally recognized claim for invasion of privacy.[35]

Thus, to a large extent, the lawfulness of a warrantless search or seizure by government actors (i.e., without having made a showing of

---

[26] *See, e.g.*, Denver Publ'g Co. v. Bueno, 54 P.3d 893, (Colo. 2002). (The tort labeled "false light invasion of privacy" recognizes a civil cause of action for injuries caused by publication of information that places the plaintiff in a "false light," which is recognized in some jurisdictions, but rejected in others as being essentially duplicative of defamation.)

[27] RESTATEMENT (SECOND) OF TORTS § 652B (AM. L. INST. 1977).

[28] *See id.* § 652D.

[29] *See id.* § 652B. The rules may vary, however, in a hospital setting depending on whether the patient is in an emergency situation, where medical personnel may need to search their belongings for identification, and a non-emergency situation where the expectation of privacy is higher. *See* Angela T. Burnette, *Searches of Hospital Patients, Their Rooms and Belongings*, HEALTH CARE L. MONTHLY 2, 3 (2012), available at https://bit.ly/3csPwVS.

[30] In 2019, the American Law Institute promulgated a set of principles to govern private parties' accessing, processing, and use of others' personal information. *See* Daniel J. Solove & Paul M. Schwartz, *ALI Data Privacy: Overview and Black Letter Text*, 68 UCLA L. REV. (2020), https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2722&context=faculty_publications; *see also* Press Release, Am. L. Inst., ALI Approves Principles of the Law, Data Privacy (May 22, 2019), https://www.ali.org/news/articles/ali-approves-principles-law-data-privacy/.

[31] *See* Doe v. High-Tech Inst., Inc., 972 P.2d 1060, 1072 (Colo. App. 1998).

[32] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[33] *See* The Health Insurance Portability and Accountability Act of 1996 (HIPAA) P.L. No. 104-191, 110 Stat. 1938 (1996).

[34] 42 U.S.C. § 1320d-5. For further information about the medical privacy rule, see *What Are the Penalties for HIPAA Violations?*, HIPAA J. (Jan. 15, 2021), https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/.

[35] *See supra* notes 24–25.

probable cause before a judge) or an intrusion or disclosure of information by private actors, turns on whether the physical or virtual space intruded upon, or the personal information disclosed without consent is subject to an objectively reasonable "expectation of privacy," a key concept that will be discussed in further depth below.

Before I begin the effort to "chart the stars," I admit the limited *practical* utility of geo-spatial matrix I delineate below. Even if one accepts that the indices I articulate are the appropriate metrics against which any particular data mining and analysis technology is to be assessed, the proper placement of any particular technology/application in that defined universe would, unquestionably, require consideration of other highly individualized factual inquiries:

(1) what does the particular technology do, i.e., "how does it work?";[36]

(2) what are the technology's capabilities of eliciting information about an individual, especially when combined with other available data points?;

(3) how commonplace is the technology in practice (is it in widespread, common usage, or relatively obscure/deployed only in rare circumstances)?;

(4) to whom is the technology being applied?;

(5) *by whom* is the technology being used (e.g., government vs. private actors)?;[37]

[36] For an explanation of how FRT works, see Scott, *supra* note 1.

[37] *See, e.g.*, Sanders v. Am. Broad. Co., 978 P.2d 67, 74 (Cal. 1999) ("decisions discussing . . . expectations of privacy against government searches are not directly applicable to the common law privacy tort context"); *see also* Desnick v. Am. Brod. Cos., 44 F.3d 1345, 1353 (7th Cir. 1995) (plaintiff's reasonable expectation of privacy does not depend on whether any intrusion thereon is committed by undercover government testers rather than by undercover news reporters). Several organizations have promulgated guidelines for FRT use by private actors. *See, e.g.*, U.S. Dept. of Comm. Nat'l Telecom. & Info. Admin., PRIVACY BEST PRACTICES RECOMMENDATIONS FOR COMMERCIAL USE OF FACIAL RECOGNITION (June 17, 2016), https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2016/06/privacy_best_practices_recommendations_for_commercial_use_of_facial_recogntion.pdf; FUTURE OF PRIVACY FORUM FOR FACIAL RECOGNITION TECHNOLOGY IN COMMERCIAL APPLICATIONS (Sept 2018), https://fpf.org/wp-content/uploads/2019/03/Final-Privacy-Principles-Edits-1.pdf; U.S. CHAMBER OF COM. TECH. ENGAGEMENT CTR. FACIAL RECOGNITION POLICY PRINCIPLES (Dec. 2019), https://www.uschamber.com/sites/default/files/ctec_facial_recognition_policy_principles_002.pdf.

(6) what is the margin of error (e.g., what is the rate of "false positives" and "false negatives)?[38]; and

(7) to what extent does that error rate differ among various sectors of the human population?[39]

Before any particular application or technology could be properly plotted onto the rubric I describe below, each of these questions would need full explication.

D. The Indices Described

My visual conceptualization is defined by three intersecting axes, each of which represents a continuum from "zero or negligible" to "complete/total": (1) degree of express or implied consent, (2) degree of personal revelation, and (3) magnitude of consequence. I will explain each of these below, prior to plotting a handful of judicial precedent "stars" in the constellation.

I concede, however, that there is a fair amount of overlap among, and interplay between, the three indices, i.e., they are not mutually exclusive; instead, each index is influenced by and dependent upon the other two. For example, the degree to which one "consents" to have his or her face photographed in a public place–which historically has been understood as complete or total consent–may be altered. For example, upon being informed that by showing one's face in public, on a street, or on the internet, one is relinquishing to others *all information associated with that person's identity*, one might choose to withdraw his or her face from public view by donning a full-face mask[40] or a disguise, to maintain control over disclosure of the myriad data points associated with his or her distinctive facial features.[41]

---

[38] *See, e.g.*, Claire Reilly, *Facial-Recognition Software Inaccurate in 98% Of Cases, Report Finds*, CNET (May 13, 2018), https://www.cnet.com/news/facial-recognition-software-inaccurate-in-98-of-metropolitan-police-cases-reports/.

[39] For example, one study found that among commercial vendors of FRT software, false positives are up to 100 times more likely for Asian and African American faces when compared to White faces. PATRICK GROTHER, MEI NGAN, & KAYEE HANAOKA, NAT'L INST. OF STANDARDS AND TECH., FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[40] Note, however, that this may not be enough to hinder sophisticated FRT. *See* Masha Borak, *Wearing a Mask Won't Stop Facial Recognition Anymore*, ABACUS (Feb. 24, 2020, 7:00 AM), https://www.scmp.com/abacus/tech/article/3052014/wearing-mask-wont-stop-facial-recognition-anymore; Carolyn Semmler, *Facial Recognition is Possible Even If Part of the Face Is Covered*, CONVERSATION (Oct. 19, 2014, 9:55 PM), https://theconversation.com/facial-recognition-is-possible-even-if-part-of-the-face-is-covered-32812 (noting that obscuring garments such as a headscarf or a hijab may actually help FRT be more accurate by covering external features like hairstyles and focusing only on the face).

[41] Justice Alito's concurrence in United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring) elucidates the circularity of the law's defining a "reasonable expectation of privacy" as dependent upon the commonality of any particular surveillance technology: "[T]he *Katz* test rests on the assumption that this

Axis 1: The Degree of Consent

It is a bedrock principle of American privacy law that individuals may consent to any intrusion thereon, and that a knowing and voluntary consent (without duress or misrepresentation) waives the right to privacy.[42] Thus, a person who provides informed and voluntary consent to a search of his home, papers, effects, or person by a government agent cannot thereafter challenge that search under the Fourth Amendment, so long as the consent was informed and voluntary.[43] The same is true of a person's knowing, voluntary disclosure of personal and private information to a private, non-governmental third party, e.g., a business, for specified uses and purposes.[44] With respect to those specifically authorized uses, the party disclosing the information to the private actor waives any causes of action for the torts of invasion of privacy.[45] By knowingly and voluntarily disclosing information (even highly personal and previously undisclosed information) to the general public, one effectively "consents" to its use by all others, regardless of who, in the general public, actually observed the person's public disclosure.[46] Accordingly, the general rule, in the United States, is that information one holds open to the general public is not subject to a "reasonable expectation of privacy."[47] Thus, it has long been understood and

hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile." *See also* Perry Keller, *The Reconstruction of Privacy Through Law: A Strategy of Diminishing Expectations*, 9 INT'L DATA PRIV. L. 132, (2019) (recognizing that the more society comes to accept intrusive technologies as the routine incidents of everyday life, the more such technologies fail to raise constitutional privacy concerns).

[42] *See* Kirsty Hughes, *A Behavioural Understanding of Privacy and its Implications for Privacy Law*, 75 MODERN L. REV. 806, 820 (2012). *See also* RESTATEMENT (SECOND) OF TORTS § 652F cmt. b (AM. L. INST. 1977).

[43] *See* Alafair S. Burke, *Consent Searches and Fourth Amendment Reasonableness*, 67 FLA. L. REV. 509, 520–21 (2016).

[44] *Voluntary Disclosure*, IGI GLOBAL, https://www.igi-global.com/dictionary/are-social-marketing-investments-used-as-a-tool-for-voluntary-reporting-or-disclosure/41332 (last visited June 6, 2021).

[45] *See* Phyllis Karasov, *Privacy*, *in* BUSINESS DISPUTES: CLAIMS AND REMEDIES (Edward T. Wahl, ed. 2019).

[46] *Id.*

[47] *See, e.g.*, Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (AM. L. INST. 1977) (declaring that there is no liability for "observing [a person] or even taking [his/her] photograph while [(s)he] is walking on the public highway, since [(s)he] is not then in seclusion, and [his/her] appearance is public and open to the public eye."); *see also* Burke v. New Mexico, Case No. 16-cv-0470 MCA/SMV, 2018 WL 2134030, at *5-6 (D.N.M. May 9, 2018) (observing that "[c]ourts routinely have found that there is no right to *privacy* in internet postings that are publicly accessible," and collecting other cases); United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012) ("When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment."); State v. Williams, 277 S.E.2d 434, 437 (N.C. 1981) (finding that a photograph taken by the police was admissible even if the defendant did not consent, because the "fourth amendment offers no shield for that which an individual knowingly exposes to public view").

accepted that one does not have a cognizable privacy interest in his or her facial image that has been voluntarily displayed in a public setting.[48]

On the polar opposite end of the consent spectrum are physical spaces or highly intimate information that the individual has steadfastly withheld from public scrutiny, like the contents of one's personal diary, medical or mental health records, or other confidential information maintained in a locked safe inside one's bedroom closet.[49] Such highly personal and private information, carefully maintained *outside* the public sphere, would undoubtedly be entitled to a strong and reasonable expectation of privacy against unauthorized access by either the government or private actors.

Axis 2: The Degree of Revelation of One's Personal Data

The second index is perhaps less obvious that the first. Its focus is not on the actual information obtained by the party who gathers it as a result of the voluntary disclosure or unauthorized intrusion into the subject's sphere of personal privacy. Instead, it examines how the party who obtains that piece of information may use it, thereafter, to determine *other information* about the subject's personal life. For example, one's social security number, a unique government-issued identifier, is of some intrinsic value to identifying an individual. But it has far greater practical utility in unlocking (accessing) a vastly greater quantum of information about the individual, particularly because that one data point has, historically, been routinely used as a unique and reliable connector to other data points.[50]

By contrast, the mere fact that an individual is White, Black, or Hispanic, male or female, thirty-five or seventy-five years old, five foot six inches versus six foot five inches tall or weighs 145 or 210 pounds–either as individual data points or, even more importantly, *in combination*–can tell us only so much about that individual's actual life experience. The fact that she or he purchased a pregnancy test, in the past week, tells us decidedly more. The fact that an individual has voted, as a registered Democrat, in each of the past twelve elections, perhaps tells us more, or at least something different, than the fact that she or he lives in a major metropolitan area, is White, and thirty-seven years old.

The more that any one data point on this continuum reveals to the recipient thereof *other* characteristics, traits, habits, predilections, and other personal experiences of that individual, the greater the degree of

---

[48] *See, e.g.*, Mark v. Seattle Times, 635 P.2d 1081, 1094 (Wash. 1981) ("On the public street, or in any other public place, the plaintiff has no legal right to be let alone; and it is no invasion of his privacy to . . . to take his photograph in such a place . . . ."); RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (AM. L. INST. 1977) (there is no "liability for observing [a person] or even taking his photograph while he is walking on the public highway, since he is not then in seclusion, and his appearance is public and open to the public eye."). Nor does publishing such a photograph constitute "publicity given to private facts." Robert C. Ozer, P.C. v. Borquez, 940 P.2d 371, 377 (Colo. 1997) ("The disclosure of facts that are already public will not support a claim for invasion of privacy."); RESTATEMENT (SECOND) OF TORTS § 652D cmt. B (AM. L. INST.1977) ("[T]here is no liability for giving further publicity to what the plaintiff leaves open to the public eye.").

[49] *See e.g.*, Boyde v. United States, 116 U.S. 616, 634-35 (1886) (holding that seizing "private books and papers" might constitute an unlawful search).

[50] *See* Carolyn Puckett, *The Story of the Social Security Number*, 69 SOC. SEC. BULLETIN (Nov. 2, 2009) https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html.

intrusion upon that individual's sphere of personal privacy. And, this is true independent of consent captured by Axis 1, i.e., even if the data point(s)–one's race, gender, age, or facial features–is already in the public domain. Several of the judicial decisions discussed below make this point expressly.

At least one previous commentator has recognized that "not only the initial acquisition of evidence, but also the latter use of evidence can affect the reasonableness of a search and seizure" under the Fourth Amendment.[51] Thus, there are two "examples of the Court considering *the subsequent use of* information or evidence when determining reasonability under the Fourth Amendment."[52]

Axis 3: The Potential Consequences of the Data's Use by a Third Party

The final of the three indices is the most contextual and the most practical. It looks at what the person whose information is obtained by third parties stands to lose from those third parties' obtaining or use of that information. Another shorthand for this metric is "the stakes": what is *at stake* to the subject person if the information is obtained by third parties? Is it possible that she or he will not be admitted into a college dorm, without some other form of identification? Will she or he not be able to purchase food in a college cafeteria without a meal plan card in hand? These incursions on the liberty of the subject might not warrant significant concern with the ease of third-party access to the data upon which those incursions are based. But that calculus changes as the consequences of unconsented to disclosure escalate. What if, as a result of the data disclosure and analysis, the subject will be denied boarding a commercial airliner? Or she or he will be denied health insurance, a job, housing, or a bank loan? Or perhaps farthest down the continuum, she will be prosecuted for a crime, based on the data obtained by the government that is connected with the data point, and, possibly, convicted and sent to jail?

The less consequential the stakes, the less we, as a society, should be concerned with the fact that the data points at issue can be obtained without consent. But, as the examples above demonstrate, the greater the magnitude of the consequences, the greater the societal interest in whether that information is available to the government without individual consent. The related question discussed above–how accurate or inaccurate is the technology? What is the frequency of false positives?–figures ever greater as the *consequences* of error escalate.

II. CHARTING THE STARS IN THE CONSTELLATION

Having identified the three interrelated indices for determining what is a "reasonable expectation of privacy" that society is, and *should be*, willing to recognize, I will now discuss a handful of Supreme Court precedents that have applied these principles in a variety of factual and

[51] *See* Molly Bruder, Comment, *Say Cheese! Examining the Constitutionality of Photostops,* 57 AM. U. L. REV. 1693, 1724 (2008) (citing Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995) and Ferguson v. City of Charleston, 532 U.S. 67 (2001)).

[52] Bruder, *supra* note 51 at 1725. The author concludes that "Under *Vernonia* and *Ferguson*, searching the photographic database could be impermissible, even if initially taking the photograph was justified."

legal contexts. Admittedly, the vast majority of the cases below arise under the Fourth Amendment, which restricts only *the government*'s authority to conduct a "reasonable" search or seizure of information contained in one's "person[], house[], papers, and effects."[53] This is explained by the Supreme Court's constitutionally circumscribed jurisdiction, which is limited to deciding issues of *federal* constitutional or statutory law.[54] Nevertheless, the precedents discussed below help identify that parameters of the "*reasonable* expectation of privacy" that is protected by law, whether the intruder thereon is a government agent or a private actor.[55]

Any such discussion must begin with the seminal 1967 case that first articulated the "reasonable expectation of privacy" concept, *Katz v. United States*.[56] The question presented was whether the planting of an audio recording device on the outside of a public phone booth, by government agents, *without a search warrant*, for the purpose of capturing and recording the phone conversation of one individual (Katz) inside that phone booth, violated his rights under the Fourth Amendment. The Court ruled that the planting of the listening device had intruded on Katz's "reasonable expectation of privacy," even though there had been *no physical trespass* into the closed phone booth to overhear his conversation.[57] Thus, *Katz* holds that a person can possess a "reasonable expectation of privacy" in information she or he discusses "in a public place"–a glass phone booth on a city street–so long as her expectation that *the information at issue* will not be overheard or intercepted by others is a reasonable one:

> [W]hat [Katz] sought to exclude when he entered the [phone] booth was not the intruding *eye* – it was the uninvited *ear*. He did not shed his right to do so simply because he made his calls from a place where he might be seen. . . . One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.[58]

Nevertheless, in *Katz*, the Court made clear that a person does not enjoy a "reasonable expectation of privacy" in information that she or he "knowingly exposes to the public."[59] To expose information to the public is to waive any claim to a "reasonable expectation of privacy" in that information.[60] Thus, the clothing that Katz was wearing in the glass phone booth, and *his facial features*, were *not* subject to a reasonable expectation of privacy; but the contents of his conversation over the phone were.

Ah, but remember: "consent" is only one of three indices in the matrix. Things become more complicated, I maintain, when the

---

[53] U.S. CONST. amend. IV.

[54] *See About the Supreme Court*, U.S. CTS., https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/about (last visited June 6, 2021).

[55] *See* Kamin, *supra* note 13 (discussing the distinction between governmental and non-governmental violators of privacy).

[56] 389 U.S. 347 (1967).

[57] *Id.*

[58] *Id.* at 352 (emphasis added).

[59] *Id.*

[60] *Id.*

information freely disclosed to the public can be used to discover or derive other information about an individual that she or he has not left open to public view.

A. Enter the Computer Age

Perhaps the earliest articulation of the dangers that massive computer databases and digitized analysis of data pose to the sphere of personal privacy came a decade after *Katz*, in the 1977 case of *Whalen v. Roe*.[61] There, the Court was asked whether a New York state statute that required recipients of welfare benefits to submit, and for the state to maintain in a database, all medical prescriptions the recipient received while on the public dole, violated those recipients' rights under the Fourteenth Amendment's protection for the right of privacy.[62] A unanimous Supreme Court held that state's record keeping regime was not a constitutional violation, under the particular circumstances of that statute (which included rigorous non-disclosure provisions). But in so doing, Justice John Paul Stevens, writing for the Court, made clear that:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. . . . The [government's] right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures.[63]

Justice William Brennan's separate concurrence expressed even greater concerns about the potential abuses wrought by the onset of the digital age. He wrote:

> What is . . . troubling about this scheme, however, is the central computer storage of the data thus collected. Obviously . . . collection and storage of data by the State that is, in itself, legitimate is not rendered unconstitutional simply because new technology makes the State's operations more efficient. . . . *The central storage and easy accessibility of computerized data vastly increase the potential for abuse* of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.[64]

Thus, some twenty years before the World Wide Web came into existence, or even the invention of the personal computer (with a standalone CPU), i.e., when the relatively new devices called computers were exclusively mainframes that often occupied an entire room or more,[65] the Justices recognized the dangers that rapid and efficient processing of data, including through instantaneously cross-referencing

---

[61] 429 U.S. 589 (1977).
[62] *Id.*
[63] *Id.*
[64] *Id.* at 606–07 (Brennan, J., concurring) (emphasis added).
[65] Compare this to, for example, the Apple Watch Series 6, which is the size of a postage stamp, has 36 gigabytes of storage capacity, and monitors your heart rate and blood oxygen level.

multiple related data points, posed to the reasonable expectation of privacy.

B. Computer Processing Renders "Practical Obscurity" Obsolete

The next major milestone on the road to the present state of the law came in the 1989 case, *Department of Justice v. Reporter's Committee for Freedom of the Press*.[66] This litigation arose under the federal Freedom of Information Act, when a newspaper in Pennsylvania sought, under that Act, copies of the "rap sheets"–a computerized record of all prior criminal arrests and convictions maintained by the FBI–for three members of a prominent family.[67] The lower courts upheld the Department of Justice's refusal to disclose those "agency records" citing the provisions of the federal Privacy Act, which forbids disclosures that would cause "an unwarranted invasion of personal privacy."[68]

The Supreme Court held that the Department of Justice was correct to withhold the rap sheets, notwithstanding that all of the information contained in those documents was a matter of public record. Anyone who had the time and inclination could assemble the rap sheets at issue by physically visiting each of the jurisdictions in which the three individuals had been arrested or convicted, and, upon making appropriate inquiries under state and federal freedom of information laws, obtain those records that were *compiled* and summarized in the DOJ's digitized rap sheets.[69]

In its ruling, the Court expressly recognized that the ease of access–the sheer efficiency produced by the government's compilation of other public records into the FBI's database–transformed the very nature of that information:

> Because events summarized in a rap-sheet have been previously disclosed to the public, respondents contend that Medico's privacy interest in avoiding disclosure of a federal compilation of these events approaches zero. We reject respondents' cramped notion of personal privacy. . . .
>
> . . . According to Webster's initial definition, information may be classified as "private" if it is "intended for or restricted to the use of a particular person or group or class of persons: *not freely available* to the public." Recognition of this attribute of a privacy interest supports the distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap-sheet and revelation of the rap-sheet as a whole. . . . [T]he issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. *Plainly* there is *a vast difference* between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and *a computerized summary* located in a single clearinghouse of information.[70]

---

[66] Dep't of Justice v. Reps. Comm. for Free Press, 489 U.S. 749, 780 (1989) ("the privacy interest in maintaining the practical obscurity of rap-sheet information will always be high.").

[67] *Id.*

[68] *Id.*

[69] *Id.*

[70] *Id.* at 749–64.

In other words, the Court recognized for the first time that the mere connection of publicly available data points, all of which, individually, enjoyed no protection under the reasonable expectation of privacy, could be assembled into a "mosaic" of information that collectively constitutes an invasion of one's reasonable expectation of privacy.

C. Automated Tracking of an Individual's Publicly Disclosed Data Can Violate Privacy

The final two "stars" in the series of computerized data decisions involved technological means by which a party (in both cases, the government) can monitor and track the physical location of others without their consent. The first was *United States v. Jones*,[71] in which the Supreme Court found a constitutional violation occurred when a government agent placed a Global Positioning Satellite (GPS) tracking device on the outside of a criminal suspect's truck, without having obtained a judge-issued warrant to do so. Justice Scalia, writing for the majority, held the Fourth Amendment was violated not by virtue of the data the government had obtained regarding the truck driver's location, over time, but merely as a result of the physical intrusion that occurred when the agent placed the tracking device on the truck's exterior.[72]

Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, concurred separately to note that *prolonged* tracking of one's physical location, through GPS tracking, could well constitute a "search" even where there is no physical trespass on the tracked person's personal property.[73] Justice Sotomayor's separate concurrence went even further:

> In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. . . . The Government can store such records and efficiently mine them for information years into the future. . .
>
> Awareness that the Government may be watching chills associational and expressive freedoms. And *the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse* . . . [B]y making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track–may "alter the relationship between citizen and government in a way that is inimical to democratic society."
>
> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.[74]

---

[71] 565 U.S. 400 (2012).

[72] *Id.* at 407.

[73] *Id.* at 418-31 (Alito, J., concurring).

[74] *Id.* at 415-16 (Sotomayor, J., concurring) (citations removed). Justice Sotomayor noted that GPS data could reveal various intimate details about the tracked

Thus, Justice Sotomayor recognized that the government's automated collection of unquestionably public information–the whereabouts on public streets of the suspect's vehicle–which could be manually recorded by the police had they tailed the truck, without any need for a warrant, can give rise to a violation of one's reasonable expectation of privacy.[75]

The second location-tracking case was decided six years later in *Carpenter v. United States*.[76] In that case, the Justices were asked whether the government's collection of another criminal suspect's location data spanning six days, via cell phone tower data obtained without a warrant from the suspect's phone carrier, violated his reasonable expectation of privacy.[77] The Justices recognized that the data points collected were more intrusive than those at issue in *Jones*:

> Unlike [the GPS tracker affixed to the] car in *Jones*, a cell phone–almost a feature of human anatomy, tracks nearly exactly the movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner *beyond public thoroughfares and into private residences*, doctor's offices, political headquarters, and other potentially revealing locales.[78]

The Court ruled 5-4, that a "search" of Carpenter's physical location data without a warrant violated the Fourth Amendment, even though he had voluntarily disclosed that data to his third-party telephone service provider.[79] Thus, *Carpenter* brought to fruition Justice Brennan's incisively prescient musings, some 40 years earlier, that perhaps "future developments will. . . demonstrate the necessity of some curb on such [data mining] technology."[80] In 2018, the Justices expressly declared that the computer-processed compiling and analyzing of data points that one had voluntarily exposed to third parties *can* give rise to a violation of subject's reasonable expectation of privacy in such data.

D. New, and Relatively Obscure, Invasive Technologies Pose Special Concerns

Another case in this area of law worth considering directly addressed whether people have a reasonable expectation of privacy in not having their homes–as opposed to their papers, persons, or effects–invaded and searched via high-tech devices. In *Kyllo v. United States*,[81] the Supreme Court held it was a violation of a homeowner's rights under the Fourth Amendment to have been subjected to a warrantless search of the interior of his home by government using a thermal imaging device to determine the presence of high-intensity heat lamps commonly used in

---

individual, including "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."

[75] *Id.*
[76] 138 S. Ct. 2206 (2018).
[77] *Id.* at 2213.
[78] *Id.* at 2218.
[79] *Id.* at 2223.
[80] Whalen v. Roe, 429 U.S. 589, 607 (1977) (Brennan, J., concurring).
[81] 533 U.S. 27 (2001).

the industrial growing of marijuana.[82] Of course, like in *Katz*, the police had not *physically* intruded or trespassed on the sanctity of the home, any more than they had with respect to Katz's phone booth. Instead, the thermal imaging scanner allowed the government to "see" activities inside the home, notwithstanding that the window shades were drawn and no person standing on the sidewalk beside the home could observe what was going on inside.

As the Court aptly characterized the issue: "[t]he present case involves officers on a public street engaged in more than naked-eye surveillance of a home. We have previously reserved judgment as to how much technological enhancement of ordinary perception from such a vantage point, if any, is too much."[83] Ultimately, the Court concluded that the technological advance applied in that case–permitting the government agents outside the home to *virtually* "see" what was happening inside the home–constituted a search for which a warrant was required: "[w]e think that obtaining by sense-enhancing technology *any information* regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, constitutes a search–at least where (as here) the technology in question is not in general public use."[84]

But, of course, the sanctity of the home as a quintessential "zone of personal privacy" was a cornerstone of that ruling: "[i]n the home, our cases show, all details are intimate details, because the entire area is held safe from prying government eyes."[85] Thus, the Court might look differently on a futuristic *Star Trek*-like medical scanner device that can peer inside the human body, like today's room-size MRI scanners, to monitor, gauge, and observe internal bodily functions or other intimate information.

E. Government Restrictions on Publication/Use of Publicly Available Truthful Information

One final set of cases also bear discussion in contemplating whether local, state, or federal statutes may constitutionally impose restrictions, with attendant consequences for violation, including civil damages and/or criminal penalties, on the use of information that is in the public domain.[86] In a series of cases dating back to 1979, the Supreme Court has repeatedly held that states, as well local authorities and the federal government, cannot impose sanctions–either civil damages

---

[82] *Kyllo v. United States*, 533 U.S. 27, 34–41 (2001).

[83] *Id.* at 33.

[84] *Id.* at 34 (internal quotation marks and citation omitted).

[85] *Id.* at 37.

[86] The Illinois Biometric Information Privacy Act is one such government restriction that has been challenged as having unconstitutional applications. *See, e.g.*, Kashmir Hill, *Facial Recognition Start-Up Mounts a First Amendment Defense,* N.Y. TIMES (Aug. 11, 2020), https://www.nytimes.com/2020/08/11/technology/clearview-floyd-abrams.html; *but see* Woodrow Hartzog & Neil Richard, *Getting the First Amendment Wrong*, BOSTON GLOBE (Sept. 4, 2020), https://www.bostonglobe.com/2020/09/04/opinion/getting-first-amendment-wrong/; Jameel Jaffer& Ramya Krishnan, *Clearview AI's First Amendment Theory Threatens Privacy–and Free Speech, Too*, SLATE (Nov. 17, 2020), https://slate.com/technology/2020/11/clearview-ai-first-amendment-illinois-lawsuit.html.

remedies or criminal penalties–upon anyone who disseminates (a) truthful information, (b) that was lawfully-obtained, and which (c) addresses a matter of legitimate public interest or concern, unless such sanctions are necessitated by "an overriding state interest."[87]

This doctrine, which some refer to as the Daily Mail principle, has been applied to vacate a jury verdict awarding money damages to an anonymous rape victim whose name was published in a newspaper in violation of a Florida state statute,[88] and another to a plaintiff whose illegally wiretapped conversation was broadcast by a Pennsylvania radio station in violation of the federal wiretap act, after a tape of the conversation was sent, anonymously, to the radio station.[89] In explaining why the wiretap victim's privacy interests did not present a sufficiently weighty interest to justify punishing the innocent recipient and publisher of that information, the Court reasoned:

> [W]e acknowledge that some intrusions on privacy are more offensive than others, and that the disclosure of the contents of a private conversation can be an even greater intrusion on privacy than the interception itself. . . . The enforcement of [the subject statutory] provision in these cases, however, implicates the core purposes of the First Amendment because it imposes sanctions on the publication of truthful information of public concern.
>
> In these cases, privacy concerns give way when balanced against the interest in publishing matters of public importance.[90]

Another application of First Amendment restraint on government regulation of information dissemination came in 2011, when the Supreme Court struck down a Vermont statute that prohibited only pharmaceutical companies with attendant monetary fines from disseminating patients' de-identified prescription drug records maintained by state regulators.[91] The Court made clear that "restrictions on the disclosure of government-held information can facilitate or burden the expression of potential recipients and so transgress the First Amendment."[92] Ultimately, the Court found the Vermont statute was insufficiently narrowly tailored and neutral in its treatment of differently situated speakers to withstand heightened judicial scrutiny. As the Court stated:

> The capacity of technology to find and publish personal information, including records required by the government, presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure. In considering how to protect those interests,

---

[87] *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514, 527 (2001) ("As a general matter, state action to punish the publication of truthful information seldom can satisfy constitutional standards. . . . More specifically, this Court has repeatedly held that if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need . . . of the highest order.") (internal quotations and citations omitted).

[88] Florida Star v. B.J.F., 491 U. S. 524 (1989).

[89] *Bartnicki,* 532 U.S. at 535.

[90] *Id.* at 533–34.

[91] Sorrell v. IMS Health Inc., 564 U.S. 552 (2011).

[92] *Id.* at 569.

however, the State cannot engage in content-based discrimination to advance its own side of a debate.[93]

F. Will Such First Amendment Concerns Apply to Government Regulation of Facial Recognition Technology?

Unlike the Vermont statute struck down in *Sorrell*, the Illinois Biometric Privacy Act applies equally to all parties who obtain or distribute protected information without the subject's consent.[94] Thus, it does not suffer from the same "discrimination among speakers" deficiency that rendered the Vermont statute unconstitutional. However, the Illinois Act does not appear, on its face, to draw any distinction between biometric data that has already been exposed to public scrutiny, and hence, is "lawfully obtained" by anyone who scrapes or downloads the publicly available data, and that which has not been so exposed, i.e., truly "private" information. In that regard, the statute would appear vulnerable to a facial constitutional challenge under the Daily Mail principle and, depending on the particular circumstances, a potential "as applied" challenge as well.

It remains an open question whether sophisticated computerized processing and analysis of facial images intentionally left open to the public view, when combined with other data sets in a way that reveals highly personal information, will render the uses of those images by state or private actors qualitatively different, and therefore "unlawfully obtained," like the arrest records in *Dep't of Justice v. Reps. Comm.* or the prolonged tracking of whereabouts through cellphone data in *Carpenter*. If compilation and use of this information is found *not* to be on a matter of public significance, or to have been obtained unlawfully, it could be removed from the shelter of the Daily Mail principle.

CONCLUSION

This essay has canvassed a set of measuring sticks that courts have utilized in deciding whether a new (or improved) technology intrudes upon individuals' reasonable expectation privacy. The three metrics I propose above are not mutually exclusive, nor, candidly, sufficiently linear to enable configuration into a neat and tidy three-dimensional matrix. Even if the metrics define nothing more than a polymorphic, irregularly shaped mapping of the legal landscape, I hope it is one that will provide a frame of reference for past, present and future such technologies, and their uses.

My effort to chart the stars in the data privacy constellation has made me appreciate, more than I had previously, the complexity and ambiguity of the interaction between the various indices and the ever-evolving notion of what we, as a society, believe constitutes a *reasonable* expectation of privacy, which Justice Harlan, in his concurrence in *Katz*, defined as "one which society is prepared to recognize as 'reasonable.'"[95] While I would not venture to predict the outcome of any particular case or controversy, pending now or in the future, my travel among these

---

[93] Sorrell v. IMS Health Inc., 564 U.S. 552, 578–80 (2011).
[94] 740 ILL. COMP. STAT. 14/ (2008).
[95] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

celestial signposts has caused me to doubt the simplistic notion that "any information that is freely left open to the public" can be harvested, compiled manipulated, processed, and analyzed, *ad infinitum*, including through sophisticated computerized operations, without raising any concerns regarding the personal privacy of the persons who "consented" to releasing only that one data set to the public. Only time will tell how the courts will chart the recently re-discovered "star" known as Facial Recognition Technology, and, after that, whatever is the "next big thing" in data collection, processing and analysis.