Maine Law Review

Volume 73 | Number 2 Article 2

June 2021

The Development and the Future of Privacy in Maine

Scott P. Bloomberg
University of Maine School of Law

THE DEVELOPMENT AND THE FUTURE OF PRIVACY LAW IN MAINE

Scott Bloomberg

THE DEVELOPMENT AND THE FUTURE OF PRIVACY LAW IN MAINE

Scott Bloomberg[*]

ABSTRACT

In the United States, privacy law has traditionally developed in concert with intrusions created by newfangled technologies. This pattern has held true in Maine. Beginning in the late 1960s, the state has experienced three eras of privacy reform that track the technological advances of the mid-century, the internet era, and the new era of social media and big data. This Article details these eras of reform and advances several proposals for responding to the challenges posed by the present era.

Indeed, at the beginning of the 2020s, there is much work on the horizon to ensure that Maine's privacy laws keep up with new technological and social developments. The coronavirus pandemic looms large over all facets of society and privacy law is no exception. The pandemic had made us even more reliant on online services that collect, use, and share previously unfathomable quantities of data, leaving residents' personal information vulnerable to misuse. Increased attention to racial injustice and over-policing in the wake of George Floyd's tragic murder have likewise highlighted privacy issues with which Maine must continue to grapple. Finally, Northeastern University recently opened the Roux Institute in Portland, offering various graduate-level degrees pertaining to the practical application of artificial intelligence and machine learning in the digital and life sciences. This development offers exciting educational and economic opportunities for the state, but also indicates that regulating AI and machine-learning technologies will be important to preserving Mainers' privacy rights in the near future. All of these recent challenges, moreover, have emerged against the backdrop of the existing privacy threats posed by social media, big data, mass surveillance, and more.

This Article is thus well-timed to inform those who will be tasked with shaping Maine privacy law in the coming years and decades. In Part II of the Article, I detail the three eras of reform highlighted above. In Part III, I propose that Maine enact a general consumer privacy law endowing Mainers with certain rights to their personal information, vesting consumer privacy rulemaking authority in a state agency, regulating automated decision-making technologies, and more. After proposing the general consumer privacy law, I identify five privacy threats that warrant additional attention from the legislature: facial recognition technology; biometric information; smart-home devices; data brokers; and the Maine Information and Analysis Center. Part IV briefly concludes the Article.

---

*Associate Professor of Law, University of Maine School of Law. I thank Cindy Hirsch for her excellent research assistance with this project, Stephen Stich and Brendan McQuade for their input on earlier drafts of this paper, the staff of the Maine Law Review for their superb editorial work, and Maine State Rep. Maggie O'Neil for introducing legislation that adopts many of this paper's recommendations. Any errors are my own. As always, I owe the deepest debt of gratitude to my wife, Amber, without whose support this paper would not have been possible. Finally, I dedicate this Article to my daughter, Lyla. May you grow up in a society that safeguards your privacy.

I. INTRODUCTION

The body of privacy law in the United States is a mosaic of reforms enacted in response to privacy intrusions posed by technological advances. This was true from the body's ostensible birth in 1890, when Samuel Warren and Louis Brandeis argued for a right to privacy in light of the new cameras that had "invaded the sacred precincts of private and domestic life," and the "numerous mechanical devices" that threatened to "make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[1] By the 1960s, advances in technology promised to expose even the most intimate areas of life. Gadgets like hidden cameras and discreet recording devices allowed eavesdroppers to capture conversations and images without being noticed, while inventions like the polygraph, personality tests, and subliminal messaging threatened to reveal the mind's inner-workings.[2] Local governments, state governments, and the federal government responded to these new technologies by adopting reforms that are now considered foundational to privacy law.[3]

The expansion of the internet and mass-computing in the 1990s led to a multitude of new privacy issues regarding personal information. Details once considered beyond public reach could be accessed, searched, organized, and stored by anyone with a desktop and a dial-up connection. Threats to privacy caused by our new connectivity stirred legislatures to adopt laws governing unauthorized computer access, data breaches, cyber-harassment, and much more.[4] Today, the ubiquity of social media, smart devices, big data, and machine learning have accelerated the privacy concerns attendant to computers and the internet that began to take hold in the 1990s. Governments are still grappling with how best to respond to these new privacy risks.

This pattern of privacy law has held true in Maine. Since the late 1960s, the state has experienced three eras of privacy reform that track the technological advances of the mid-century, the internet era, and the new era of social media and big data. This Article details these three eras of reform and advances a number of proposals for responding to the challenges posed by the era that we are living through today.

Indeed, at the beginning of the 2020s, there is much work on the horizon to ensure that Maine's privacy laws keep up with new technological and social developments. The coronavirus pandemic looms large over all facets of society and privacy law is no exception. The pandemic had made us even more reliant on online services that collect, use, and share previously unfathomable quantities of data, leaving residents' personal information vulnerable to misuse. Increased attention to

---

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

2. *See infra* Section II(A). *See generally* ALAN F. WESTIN, PRIVACY AND FREEDOM (1967) (detailing the privacy intrusions caused by post-WWII advances in technology and legislative responses to those new advances); SARAH E. IGO, THE KNOWN CITIZEN: A HISTORY OF PRIVACY IN MODERN AMERICA (2018) (providing a history of how technology, science, and other factors have shaped American privacy norms and expectations).

3. *See infra* Section II(A) (discussing reforms pertaining to eavesdropping, consumer reports, polygraphs, and wiretapping).

4. *See infra* Section II(B).

racial injustice and over-policing in the wake of George Floyd's tragic murder have likewise highlighted privacy issues with which Maine must continue to grapple. Finally, Northeastern University recently opened the Roux Institute in Portland, offering various graduate-level degrees pertaining to "the practical application of artificial intelligence and machine learning in the digital and life sciences."[5] This development offers exciting educational and economic opportunities for the state, but also indicates that regulating artificial intelligence ("AI") and machine-learning technologies will be important to preserving Mainers' privacy rights in the near future. All of these recent challenges, moreover, have emerged against the backdrop of the existing privacy threats posed by social media, big data, mass surveillance, and more.

This Article is thus well-timed to inform those who will be tasked with shaping Maine privacy law in the coming years and decades. In Part II of the Article, I detail the three eras of reform highlighted above. In Part III, I propose that Maine enact a general consumer privacy law endowing Mainers with certain rights to their personal information, vesting consumer privacy rulemaking authority in a state agency, regulating automated decision-making technologies, and more. After proposing the general consumer privacy law, I identify five privacy threats that warrant additional attention from the legislature: facial recognition technology; biometric information; smart-home devices; data brokers; and the Maine Information and Analysis Center. Part IV briefly concludes the Article.

II. THE DEVELOPMENT OF PRIVACY LAW IN MAINE

Part II of this Article presents the first comprehensive account of the development of Maine privacy law. I have organized this account into three Sections, each tracking a wave of reform that the state enacted in response to newfangled technologies. First, I discuss the state's reforms during the late 1960s and the 1970s. These reforms include core privacy protections such as recognizing the invasion of privacy torts, criminalizing certain egregious violations of privacy, and regulating wiretapping. Second, I detail Maine's reforms during the 1990s and early 2000s, when the popularization of the internet and the personal computer ("PC") led the state to update its earlier privacy laws and to enact new ones addressing the privacy threats posed by this new form of mass communication. Third, I review Maine's more recent privacy reforms, which have primarily come in response to privacy risks posed by social media and big data.

A. The Emergence of Privacy Law in Maine

By the mid-1900s, advances in technology threatened to unveil even the most intimate areas of life. Gadgets like miniature cameras, wiretaps, and discreet recording devices—which were marketed to the public as eavesdropping tools—

5. Ian Thomsen, *Northeastern Partners with Entrepreneur David Roux to Launch the Roux Institute at Northeastern in Portland, Maine*, NE. UNIV. (Jan. 27, 2020), https://news.northeastern.edu/2020/01/27/northeastern-partners-with-entrepreneur-david-roux-to-launch-the-roux-institute-at-northeastern-in-portland-maine/ [perma.cc/6EQ3-NBEG].

allowed third parties to capture conversations and images without being noticed.[6] At the same time as the privacy of traditionally non-public spaces and conversations was being threatened, inventions like the polygraph, personality tests, and subliminal messaging threatened to reveal Americans' inner-most thoughts.[7] Risks to information privacy began to take focus during this era as well. Early data processing and computing technologies led the pioneering privacy scholar Alan Westin to warn against the privacy intrusions made possible by the collection and storage of large amounts of information about peoples' daily lives.[8]

Maine responded to these threats by enacting a series of privacy laws that often mirrored those passed in other states or at the federal level. From the late 1960s to the late 1970s, the state passed laws addressing privacy issues attendant to telephones, recording devices, wiretaps, polygraphs, private investigators, and consumer reporting agencies. Additionally, during this initial era of privacy reform in Maine, the Maine Law Court[9] recognized four invasion of privacy torts that Maine residents would come to assert in a variety of circumstances.

In 1967, Maine criminalized the "willful[], wanton[], or malicious[]" use of a telephone to transmit communications that were "obscene, lewd, lascivious, or indecent," threated to injure "person or property," or were repeated anonymous telephone calls "which disturb[ed] the peace, quiet or right of privacy of any person."[10] Maine's "Act Prohibiting Annoying Telephone Calls" made the state one of many in the country to address the privacy intrusions attendant to the widespread use of telephones in the home: telemarketers and harassers could reach into nearly anyone's home at any hour of the day or night.[11] Violations of the Act carried penalties of up to a $500 fine and eleven months' imprisonment.[12] Within two decades, almost every state in the country had similar laws on the books.[13]

---

6. *See, e.g.*, WESTIN, *supra* note 2, at 73-85 (describing various location, photography, and eavesdropping technologies in use during the 1950s and 1960s).

7. *Id.* at 158-69 (discussing government and private use of the polygraph during the 1950s and 1960s); *id.* at 145-58 (discussing government and private use of the personality tests from the 1930s through the 1960s); *id.* at 311-31 (reviewing the invention of subliminal messaging, the public response thereto, and the debate over the invention's effectiveness).

8. *See id.* at ch. 7, The Revolution in Information Collection and Processing: Data Surveillance (discussing the use of computers and data processing to create large personal dossiers and to record financial transactions, and warning of the dangers posed by the use of centralized data processing technology to create a universal credit system).

9. The Maine Supreme Judicial Court is called the "Law Court" when sitting in an appellate capacity. *See Supreme Judicial Court*, STATE OF ME. JUDICIAL BRANCH, https://www.courts.maine.gov/courts/sjc/index.html [https://perma.cc/NC79-TTRT] (last visited Apr. 11, 2021).

10. Me. P.L. 1967, ch. 176.

11. *See* Andrea J. Robinson, Note, *A Remedial Approach to Harassment*, 70 VA. L. REV. 507, 522-24 & n.75 (1984) (discussing statutes directed at combating telephonic harassment and noting that by 1964 American Law Reports had published an annotation on misuse of the telephone as a minor criminal offense).

12. Me. P.L. 1967, ch. 176.

13. *See* Mark S. Nadel, *Rings of Privacy: Unsolicited Telephone Calls and the Right of Privacy*, 4 YALE J. ON REGUL. 99, 106 (1986) ("Forty-five states have laws that prohibit harassment by telephone calls made with the purpose, intent, or knowledge that the call will annoy."). Another account from 1984 concludes that every state had laws prohibiting "at least some types of telephone misuse." Robinson, *supra* note 11, at 522 & App. Many telephone harassment laws were declared unconstitutional based on First Amendment overbreadth or vagueness concerns, although courts are

Maine significantly revised the state's annoying telephone calls law when the legislature enacted Maine's criminal code in 1975. Section 506 of the code prohibited harassment "by means of telephone," and perhaps in response to constitutional challenges to similar laws in other states, provided a more tailored definition of that crime than did the 1967 Act.[14] The revised law prohibited, *inter alia*: obscene calls made "without consent of the person called"; anonymous calls made "with intent to annoy, abuse, threaten, or harass"; and repeated calls made with intent to harass.[15]

Around the same time as Maine was adopting protections for recipients of annoying or harassing phone calls, the state also acted to protect those whose calls were being intercepted by third parties. In 1973, Maine followed the federal government and several other states in enacting the Interception of Wire and Oral Communications Act.[16] The Act protected the privacy of telephone (wire) and in-person (oral) communications by criminalizing the interception of both types of communications.[17] As a prophylactic measure to guard against this core privacy protection, the Act also prohibited the willful disclosure or use of communications known to have been unlawfully intercepted, as well as the possession and sale of devices used for intercepting wire and oral communications.[18] And, the Act imposed an affirmative duty on telephone companies to report potential violations of the law.[19]

The legislature enacted two significant privacy reforms during this era that extended beyond the confines of privacy intrusions caused by misuse of the telephone and to the realm of physical invasions of privacy. First, in 1971 the state passed a law to regulate "professional investigators," perhaps more commonly

---

generally divided on the constitutionality of such statutes. *See generally* M. Sean Royall, Comment, *Constitutionally Regulating Telephone Harassment: An Exercise in Statutory Precision*, 56 U. CHI. L. REV. 1403 (1989) (reviewing courts' treatment of laws criminalizing annoying or harassing telephone calls under the First Amendment); Wayne F. Foster, *Validity, Construction, and Application of State Criminal Statute Forbidding Use of Telephone to Annoy or Harass*, 95 A.L.R.3d 411 (originally published in 1979) (collecting cases).

14. An Act Creating the Maine Criminal Code, Me. P.L. 1975, ch. 499, § 1 (codified as amended at 17-A M.R.S.A § 506(1)).

15. *Id.*

16. Me. P.L. 1973, ch. 561 (codified as amended at 15 M.R.S.A. §§ 709-712); *see also* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, § 802, 82 Stat. 197, 212 (creating Chapter 119 of title 18 of the U.S. Code, titled "Wire Interception and Interception of Oral Communications"); WESTIN, *supra* note 2, at 179-91 (discussing state wiretap reform laws in the 1950s and 1960s). Maine's prohibition on intercepting oral and wire communications contained certain exceptions applicable to law enforcement and telephone companies. *See* Me. P.L. 1973, ch. 561 (codified as amended at 15 M.R.S.A. §§ 710, 712).

17. *See* Me. P.L. 1973, ch. 561(codified as amended at 15 M.R.S.A. § 710) (criminalizing the willful interception or attempted interception of oral or wire communications).

18. *See id.* The Act's prohibitions are similar to the prohibitions contained in its federal counterpart. *See* § 802, 82 Stat. at 212. The scope of the Act's prohibitions and exceptions have been modified since their original enactment, but remain largely the same as when they were originally enacted in 1973. *See* 15 M.R.S. § 710 (2013) (using a "knowingly or intentionally" standard rather than a "willfully" standard and including certain exceptions for investigative officers and Department of Corrections employees).

19. Me. P.L. 1973, ch 561 (codified as amended at 15 M.R.S.A. § 710(4)) (imposing a duty to report on communications common carriers).

known as private investigators or "P.I.s." By the late 1960s, approximately 20,000 Americans were employed as P.I.s working for "their own firms, for large detective agencies, for insurance and credit companies, or as corporate security officers."[20] Device manufacturers "aggressive[ly] promot[ed]" equipment such as "tapping devices, miniature microphones, and cameras" to P.I.s, who purchased these devices to surveil their targets.[21] This technology gave P.I.s the ability to hide listening devices in objects as small as "cigarette lighters, clasps of ladies' handbags and cigarette packs; two-inch 'palm' cameras; and similar equipment."[22] P.I.s also compiled personal information about their subjects by speaking to their subjects' neighbors. "Suburbia was a treasure trove of information for those with a financial stake in personal 'character' and habits . . . so agents roamed residential neighborhoods in search of peers who would talk."[23]

The growth of the P.I. industry and investigators' use of such intrusive devices contributed to the genuine—and justified—paranoia about who may be watching, listening, or snooping on Americans.[24] This paranoia led to both the enactment of state laws regulating private investigators and to the wiretapping laws discussed above. Maine's P.I. law, "An Act Relating to the Regulation of Private Detectives," imposed a licensing requirement on P.I.s and prohibited P.I.s from taking certain actions to disrupt or incite labor strikes, interfere with labor negotiations, or attempt to break-up labor unions.[25] Today, forty-five states have laws regulating and licensing P.I.s.[26]

Second, the state created a violation of privacy crime in 1975.[27] The law was designed to protect the privacy of people while they were in "private places," defined to mean "a place where one may reasonably expect to be safe from surveillance."[28] The legislature accordingly made it a crime to trespass on property "with intent to overhear or observe any person in a private place," to install or use "any device for

---

20. WESTIN, *supra* note 2, at 97.

21. *See id.* at 98.

22. *Id.*

23. IGO, *supra* note 2, at 114.

24. *See, e.g.*, *id.* at 114 ("The sudden uptick in the use of private investigators (in the 1950s) was of special concern.").

25. *See* Me. P.L. 1971, ch. 582, § 1 (codified as amended at 32 M.R.S.A. § 3809 (repealed 1977)) (listing prohibited conduct).

26. *See State-by-State Private Investigator Licensing Requirements*, PURSUIT MAG., https://pursuitmag.com/resources/investigator-licensing/ [https://perma.cc/5UFG-SPVY] (last visited Nov. 15, 2020) (compiling state licensing requirements).

27. An Act Creating the Maine Criminal Code, Me. P.L. 1975, ch. 499 (codified as amended at 17-A M.R.S.A.). For an overview of state laws criminalizing similar invasions of privacy, see Lance E. Rothenberg, Comment, *Re-Thinking Privacy: Peeping Toms, Video Voyeurs, and Failure of the Criminal Law to Recognize a Reasonable Expectation of Privacy in the Public Space*, 49 AM. U. L. REV. 1127, 1142-44 (2000), noting that "the criminalization of privacy intrusion is firmly established in many state penal codes, falling under a wide variety of crimes," and collecting state statutes regarding different types of privacy intrusions.

28. Me. P.L. 1975, ch. 499, § 1 (codified as amended at 17-A M.R.S.A. § 511). The definition of "private place" exempted "a place to which the public or a substantial group has access." The law thus did not protect the privacy of conversations that occurred in places like bars and restaurants, even if it would have been reasonable to expect privacy from surveillance in such places. As discussed *infra* Section II(B), the legislature would remove this exception and revise the definition of "private places" decades later.

observing, photographing, recording, amplifying or broadcasting sounds or events" in private places without consent, and to install or use *outside* of a private place devices designed for "hearing, recording, amplifying or broadcasting sounds originating" from the private place.[29]

The state also acted to regulate the use of polygraphs, which not only posed challenging problems for criminal procedure[30] but were also commonly used to pry and embarrass women and suspected homosexuals about their intimate thoughts and behaviors. By the 1960s, polygraph testing was widely used by police departments and federal agencies for investigative purposes.[31] Commercial uses of the polygraph had grown in popularity too. Beyond using polygraphs to investigate commercial crimes such as embezzlement, companies and government employers required prospective employees to take polygraph exams and subjected existing employees to periodic polygraphs to deter misconduct.[32] Tests were given in the employment context to vet employees for promotions, assess employee attitudes about co-workers, and to determine how happy workers were with their jobs.[33] Government employees, and employees of government contractors, were additionally subjected to "loyalty checks" using polygraph machines.[34]

The content covered in these tests was wide-ranging and intrusive. For example, in the 1950s the National Security Agency ("NSA") made it a practice to use an "Embarrassing Personal Question" or "EPQ" technique to vet prospective employees.[35] Common questions directed to women reportedly included "[h]ave you ever slept with a man?" and "[d]id you sleep with your husband before you were married?"[36] During Congressional hearings on the use of polygraph examinations in 1964, one congressman recounted the story of a seventeen-year-old typist at the NSA, who "became quite disturbed when she was asked a series of questions about homosexual activity by the male operator administering the test while the two were alone in the polygraph examining room."[37] Private-sector employers abused the new technology as well, using polygraph tests to ask employees about "union activities,

---

29. Me. P.L. 1975, ch 499, § 1 (codified as amended at 17-A M.R.S.A. § 511). The statute exempted people acting "in the execution of a public duty or as authorized by law." *Id.* § 1 (codified as amended at 17-A M.R.S.A. § 511(1)).

30. As early as 1954, the Law Court had "consistently ruled that not only are polygraph tests inadmissible, but also that evidence that a defendant agreed to take a polygraph test, or refused to take such test, is not admissible." State v. Bowden, 342 A.2d 281, 283 (Me. 1975) (citing State v. Casale, 110 A.2d 588 (Me. 1954); State v. Mottram, 184 A.2d 225 (Me. 1962); State v. Mower, 314 A.2d 840 (Me. 1974)).

31. *See, e.g.*, WESTIN, *supra* note 2, at 158-59 (estimating that over half of the police departments in the United States were using polygraphs and noting that in 1963 thirteen federal agencies administered a total of 12,000 polygraph tests).

32. *See id.* at 160-63 (discussing the widespread use of polygraph examinations for personnel sorting in private industry); *id.* at 164-69 (discussing how local, state, and the federal government used polygraphs for employment purposes).

33. *See generally id.* at 160-169 (discussing the polygraph's use as a personnel sorter).

34. *Id.* at 161 (noting that polygraphs were used by government contractors to administer polygraph examinations); *id.* at 165-67 (summarizing a polygraph examination given to a prospective NSA employee that probed the subject's sympathies toward communism).

35. *Id.* at 167.

36. *Id.*

37. *Id.* at 168.

personal finances, past employment and future job plans, drinking habits, physical condition, police record, driving habits, sexual activities, and political beliefs."[38]

These disturbing abuses led states to begin restricting the use of polygraph tests. By 1966, ten states had banned the use of polygraphs as a condition of employment, while six other states had enacted licensing requirements for polygraph examiners.[39]

Maine followed these early-moving states in 1979 by enacting the "Act to Establish Registration of Polygraph Examiners."[40] The Act made it unlawful for polygraph examiners to "ask any questions pertaining to sexual behavior of any type or questions that could be construed as being sexually oriented," to "probe the political or religious beliefs of any individual," and to "subject a person to a polygraph examination without that person's full knowledge and consent."[41] The Act further prohibited the use of polygraphs for preemployment screening and for employment purposes.[42] The grounds for revoking or suspending a license provided additional privacy protections for subjects of polygraph examinations.[43] Examiners were subject to penalties against their license for failing to disclose the nature of the examination and the specific questions to be asked; that the examination was voluntary; that the subject had rights to refuse and terminate the examination; that the subject had a constitutional right against self-incrimination; for asking prohibited sexual questions; for not giving the subject an opportunity to offer explanations for their responses; for conducting an examination to interfere with or prevent the lawful activities of a labor union; and more.[44]

Toward the end of this initial era of privacy reform in Maine, the legislature enacted the Maine Fair Credit Reporting Act ("Maine FCRA"), the first law in the state that attempted to tackle privacy intrusions caused by the amassing and analysis of large quantities of personal information by the private sector.[45] By the 1970s, advances in computing and data-processing technologies had allowed commercial actors to collect and compile information files on consumers for use in determining credit-worthiness, insurability, eligibility for employment, and more.[46] The agencies

---

38. *Id.* at 243.

39. *See id.* at 244, 251 (noting that by 1965, Massachusetts, Oregon, Rhode Island, California, Washington, and Alaska had banned the use of polygraph tests in employment, while New Jersey, Maryland, Hawaii, and Delaware followed suit in 1966); *id.* at 246 (stating that Illinois, Kentucky, New Mexico, North Dakota, and Texas had established licensing laws by 1966).

40. An Act to Establish Registration of Polygraph Examiners, Me. P.L. 1979, ch. 209, § 2 (codified as amended at 32 M.R.S.A. §§ 7351-7390).

41. *See id.* (codified as amended at 32 M.R.S.A. § 7154). The prohibition on asking sexual questions contains exceptions for certain criminal investigations and civil litigation where sexual behavior is at issue. *Id.*

42. *Id.* (codified as amended at 32 M.R.S.A. § 7166).

43. *Id.* (codified as amended at 32 M.R.S.A. § 7161).

44. *Id.*

45. An Act to Establish the Fair Credit Reporting Act, Me. P.L. 1977, ch. 514, *amended by* An Act to Clarify and Define Certain Existing Provisions of the Maine Fair Credit Reporting Act, Me. P.L. 1977, ch. 677.

46. *See, e.g.*, Elizabeth D. De Armond, *A Dearth of Remedies*, 113 PENN ST. L. REV. 1, 6 (2008) (noting that in enacting the FCRA, "Congress understood how the computerization of personal information estranged individuals from their personal information, leading to a loss of control over data").

that prepared these consumer reports were largely unregulated.[47] Information from their reports could be obtained through "deliberate misrepresentation," files could contain "false or fabricated material," and consumers would have no recourse when they were denied financial services or employment based on the contents of their files.[48] Indeed, consumers were often left in the dark about what information their report contained, the basis for any adverse action taken due to information contained in the report, and even the very existence of a report.[49] Consumer reporting agencies were thus widely seen as "unaccountable gatekeepers"[50] sorely in need of regulation.

Maine took action against the consumer reporting industry in 1977, seven years after the federal government enacted the era's first and only federal law to "rein in private sector data practices"[51]: the Federal Fair Credit Reporting Act of 1970 ("Federal FCRA").[52] Finding it necessary to "insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy," Congress passed the Federal FCRA to create some basic transparency requirements and safeguards for consumers.[53] The Federal FCRA limited the purposes for which a consumer report could be used;[54] restricted agencies' use of older adverse information;[55] established requirements for disclosing information to consumers;[56] created a procedure for consumers to dispute the accuracy of information contained in a report;[57] and imposed disclosure obligations on users of reports when they made a decision adverse to the consumer based on the contents of a report.[58]

Maine's FCRA largely mirrored the federal version but provided the state's

---

47. *See, e.g.*, Christopher P. Guzelian et al., *Credit Scores, Lending, and Psychosocial Disability*, 95 B.U. L. REV. 1807, 1811 (2015) ("Until 1970, CRAs were unregulated. Complaints of abusive, opaque, and false estimations of creditworthiness which affected banks' and merchants' lending decisions were widespread, despite consumers' growing reliance upon credit to provide staples of daily life."); Lea Shepard, *Toward a Stronger Financial History Antidiscrimination Norm*, 53 B.C. L. REV. 1695, 1744-45 (2012) ("In passing the FCRA, Congress sought to correct key defects in the procedures by which the previously unregulated credit reporting industry operated. The industry was secretive and enigmatic. Consumers did not know when and by whom their credit reports were being utilized. Consumers had no access to their consumer reports. In addition, they could not correct incomplete, irrelevant, or obsolete information.").

48. IGO, *supra* note 2, at 229.

49. *See, e.g.*, Shepard, *supra* note 47, at 1745 (describing consumer reporting agencies' poor practices and commenting that "job applicants had no idea that adverse and frequently erroneous or subjective information in their consumer reports might be 'controlling their troubled careers'").

50. IGO, *supra* note 2, at 229.

51. *Id.* (referring to the FCRA as the era's only law regulating private-sector data practices).

52. *See* Equifax Servs., Inc. v. Cohen, 420 A.2d 189, 192-94 (Me. 1980) (summarizing the federal and state acts and concluding that "the Maine Act paralleled the Federal Act," with some exceptions); *see also* Pub. L. 91-508, § 601, 84 Stat. 1114, 1127-36 (1970) (amending the Consumer Credit Protection Act, Pub. L. 90-321, 82 Stat. 146 (1968)).

53. Pub. L. 91-508, § 601, 84 Stat. 1114, 1128 (1970) ("Findings and purpose").

54. *Id.* § 604 (limiting use of consumer reports to credit transactions, employment purposes, insurance, certain government licenses and benefits, and other "legitimate businesses need[s]").

55. *Id.* § 605 (prohibiting consumer reporting agencies from using older information such as bankruptcies older than fourteen years old or tax liens older than seven years).

56. *See id.* §§ 606, 609, 610 (establishing several disclosure requirements).

57. *Id.* § 611.

58. *Id.* § 615(a) (requiring, in such situations, users to disclose the name and address of the consumer reporting agency and the nature of adverse information contained in a report to consumers).

residents with some additional privacy protections. As the Law Court explained in *Equifax Services v. Cohen*:

> Whereas the Federal Act requires specific notice be given to a consumer before a user can procure an "investigative consumer report,"[59] the Maine Act prohibits a user from procuring such a report until prior written authorization of the consumer is obtained. In addition, the Maine Act provides for many more absolute prohibitions against the reporting of information. Whole categories of information, such as race, religion, political affiliation and beliefs, and so forth, are classified as prohibited and to be excluded from reports. . . . Maine requires that "investigative consumer reports be written", whereas the Federal Act allows them to be oral. The Maine Act fails to confer the qualified immunity given by the Federal Act relative to consumer suits against designated persons for defamation, invasion of privacy or negligence with respect to the reporting of information.[60]

In *Equifax Services*, the Law Court reviewed a series of challenges to the Maine FCRA brought by the credit reporting agency Equifax. Maine's attempts to provide its residents with protections beyond what the Federal FCRA provided received a mixed airing. The Law Court upheld Maine's requirement that investigative consumer reports be written,[61] and it upheld the state's decision not to confer qualified immunity upon consumer reporting agencies, persons who furnish information to such agencies, and users of consumer reports.[62] However, the court found that the Maine FCRA's provision requiring users to obtain a subject's consent before using an investigative consumer report—rather than requiring the user to only notify the subject, as the Federal FCRA required—violated the First Amendment's speech clause.[63] In reaching this decision, the Law Court rejected the Attorney General's position that the government's interest in protecting privacy justified the consent requirement. The court opined that privacy is "an elusive concept," and that only particular "'zones' or 'areas'" of privacy fall within the government's "substantial" interest in protecting privacy.[64] The privacy protected by requiring users to obtain consent from the subject of a consumer report before using that report did not justify the restraints on speech imposed by the requirement.[65]

The *Equifax Services* court similarly found that the Maine FCRA's prohibition on the use of the sensitive information listed in 10 M.R.S.A. § 1321 implicated First Amendment speech rights and was not justified by a sufficient government interest.[66]

---

59. An investigative consumer report is a specific type of consumer report that includes information "bearing on a consumer's character, general reputation, personal characteristics or mode of living which is obtained through personal interviews with neighbors, friends or associates." Me. P.L. 1977, ch. 514 (codified as amended at 10 M.R.S.A. § 1312(7) (repealed 2013)).

60. Equifax Servs., Inc. v. Cohen, 420 A.2d 189, 193-94 (Me. 1980) (internal citations omitted).

61. *Id.* at 212.

62. *Id.* at 213-15.

63. *Id.* at 200 ("Section 1314(1) must be held unconstitutional because either: (1) the restraint it imposes really does not at all further a substantial governmental interest or (2) if we acknowledge that the restraint may have a degree of relation to a substantial governmental interest . . . the restraint does not directly advance that substantial interest and is more extensive than is necessary to serve it.").

64. *Id.* at 199-200.

65. *Id.* at 200.

66. *See id.* at 195 (concluding that "[s]ections 1314 and 1321 . . . [are] direct restrictions upon speech based upon the content of that speech").

Although it would be illegal for the user of a credit report to rely on some of the categories of information proscribed by section 1321—such as race and religion—in making decisions regarding creditworthiness, employment, housing, and public accommodation, it was not illegal for a consumer agency to report those characteristics.[67] Nor was it illegal for a user to be aware of those characteristics. As the court concluded, "[i]t is only when the user bases a discriminatory decision on such factors that illegal activity occurs, and nothing in evidence shows that users are generally susceptible to improper influence merely by becoming aware of them."[68]

Beyond statutory reforms, the Law Court created significant common-law protections for individual privacy during this era. In *Estate of Berthiaume v. Pratt*, the court formally recognized a "right to privacy" and declared that violation of the "legally protected right is an actionable tort."[69] In doing so, the Law Court joined a majority of other states in recognizing the four privacy torts that derive from Brandeis and Warren's seminal article, "The Right to Privacy."[70] As the court explained:

> The law of privacy addresses the invasion of four distinct interests of the individual. Each of the four different interests, taken as a whole, represent an individual's right 'to be let alone.' These four kinds of invasion are:
> (1) intrusion upon the plaintiff's physical and mental solitude or seclusion;
> (2) public disclosure of private facts;
> (3) publicity which places the plaintiff in a false light in the public eye;
> (4) appropriation for the defendant's benefit or advantage of the plaintiff's name or likeness.[71]

Plaintiffs in Maine have since asserted the torts—usually unsuccessfully in reported cases—in a range of situations, including: the unauthorized publication of an infant child's photograph;[72] portraying a corporation in false light;[73] the disclosure of settlement terms;[74] the unauthorized viewing of a woman giving birth;[75] the disclosure and use of private information during probate proceedings;[76] and

---

67. *See id.* at 203, 204-05.

68. *Id.* at 205.

69. 365 A.2d 792, 794 (Me. 1976).

70. Estate of Berthiaume v. Pratt, 365 A.2d 792, 794 (Me. 1976) (noting that a majority of other jurisdictions in the country had recognized the privacy rights); William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960) (dividing Brandeis and Warren's proposed invasion of privacy tort into four distinct torts).

71. *Estate of Berthiaume*, 365 A.2d at 795.

72. Nelson v. Me. Times, 373 A.2d 1221, 1222 (Me. 1977) (affirming dismissal of plaintiffs' claims).

73. Hearts With Haiti, Inc. v. Kendrick, No. 2:13-CV-00039, 2015 WL 3649592, at * 8 (D. Me. June 9, 2015) (finding that the Law Court would not allow a corporation to bring a false light invasion of privacy claim).

74. Loe v. Town of Thomaston, 600 A.2d 1090, 1093 (Me. 1991) (affirming dismissal of invasion of privacy claim).

75. Knight v. Penobscot Bay Med. Ctr., 420 A.2d 915, 917-18 (Me. 1980). The jury in this case found for the defendants and the Law Court affirmed the trial court's jury instructions on appeal. *Id.* at 916.

76. Bratt v. Jensen Baird Gardner & Henry, P.A., No. 2:17-CV-463, 2018 WL 4568590, at * 1 (D. Me. Sept. 24, 2018) (denying defendants' motion to dismiss).

disclosure of a person's HIV status.[77]

***

By the end of the 1970s, Maine had established basic safeguards from the intrusions on its residents' privacy posed by the technologies of the day. People who invaded the sanctity of the home through repeated or harassing phone calls or by employing discreet surveillance devices could be prosecuted under criminal laws. The state's prohibition on intercepting wire and oral communications and its regulation of private investigators, polygraph examiners, and consumer reporting agencies combined to guard Mainers against the use of intrusive, unfair, and unethical practices in collecting personal information. And, the Law Court's recognition of the four privacy torts gave Mainers civil recourse against individuals and companies who violated their right to privacy.

Within a decade, advances in technology would reveal a clear need to supplement these foundational privacy protections.

B. Reforms for the Internet Era

The expansion of the internet and mass-computing beginning around 1990 and extending through the early 2010s led to increased awareness of privacy issues regarding personal information. Information that was once considered beyond public reach was suddenly available to anyone with computer and internet access, large quantities of personal information could be readily stored in hackable electronic databases, and private information could be posted and shared on publicly available forums without the subject's consent. Maine's laws, like the laws of its sister states and the federal government, were not equipped to protect its residents' privacy interests from these new threats. The sometimes obvious shortcomings, together with well-publicized privacy intrusions from around the country, prompted the state to act. During this second era of privacy reform in Maine, the state passed laws criminalizing the unauthorized access of a computer, prohibiting cyberstalking, expanding the state's criminal invasion of privacy law, requiring businesses (and certain other persons) to report data breaches, prohibiting the sale of consumers' cell phone records, and more.

The beginning of the state's internet-era reforms can be marked by Maine's 1990 enactment of Chapter 18 of the criminal code: "Computer Crimes."[78] The Chapter included two crimes. First, a person was guilty of "criminal invasion of computer privacy" if they "intentionally access[ed] any computer resource knowing that [they

77. Stokes v. Barnhart, 257 F. Supp. 2d 288, 295 (D. Me. 2003) (dismissing the claim because the defendant only disclosed the plaintiff's HIV status to a single person).

78. Me. P.L. 1989, ch. 620. Previous versions of this bill died in the legislature after some commenters voiced concerns that the prohibitions on unauthorized computer access swept too broadly. *See An Act Relating to Computer Access*: *Hearing on L.D. 627 Before the J. Standing Comm. on Judiciary,* 114th Legis. 13-19 (1989) (detailing the opposition to a similar bill, L.D. 36 (1985)), *available from* Me. State Law & Leg. Reference Library by requesting cf114-LD-0627.pdf.

were] not authorized to do so."[79] Second, a person was guilty of "aggravated criminal invasion of computer privacy" if they knowingly: (a) copied any computer program, software, or information without authorization; (b) damaged any computer resource without having the right to do so; or (c) introduced a virus into a computer without having the right to do so.[80] At the time of enactment, at least twenty-three other states had similar laws on the books.[81]

Stalking is one of the most serious privacy intrusions people experience, and the use of computers and the internet exacerbates the problem. Beginning in 1990, states across the country began enacting laws that made stalking a specific criminal offense.[82] Although Maine had other laws, such as a law prohibiting terrorizing, that may have encompassed some stalking behavior, the state did not recognize stalking as a separate offense until 1996, becoming the last state in the nation to do so.[83] Maine's stalking statute followed the National Institute of Justice's Model Anti-Stalking Code for States,[84] criminalizing the following conduct:

> 1. A person is guilty of stalking if:
> A. The person intentionally or knowingly engages in a course of conduct directed at another specific person that would in fact cause a reasonable person:
> (1) To suffer intimidation or serious inconvenience, annoyance or alarm;
> (2) To fear bodily injury or to fear bodily injury to a member of that person's immediate family; or
> (3) To fear death or to fear the death of a member of that person's immediate family; and
> B. The person's course of conduct in fact causes the other specific person [to suffer those harms].[85]

Importantly, the statute defined "course of conduct" to encompass "gaining unauthorized access to personal, medical, financial or other identifying information, including access by computer network."[86] An interview with the bill's sponsor,

---

79. Me. P.L. 1989, ch. 620 (codified at 17-A M.R.S.A. § 432). The term "computer resources" was defined to encompass computer programs, software, systems, networks, and information. *Id.* (codified as amended at 17-A M.R.S.A. § 431).

80. *Id.* (codified at 17-A M.R.S.A. § 433).

81. *An Act Relating to Computer Access*: *Hearing on L.D. 627 Before the J. Standing Comm. on Judiciary*, 114th Leg. 6 (Me. 1989).

82. NAT'L INST. OF JUST., U.S. DEP'T. OF JUST., DOMESTIC VIOLENCE, STALKING, AND ANTISTALKING LEGISLATION: AN ANNUAL REPORT TO CONGRESS UNDER THE VIOLENCE AGAINST WOMEN ACT 1 (1996) ("The first State antistalking laws were passed in 1990.").

83. *See* Me. P.L. 1995, ch. 668, § 3 (creating the offense of stalking); NAT'L INST. OF JUST., *supra* note 82, at 7 (noting that Maine used an anti-terrorizing statute to address stalking behavior); 6 Legis. Rec. H-1857 (2d Reg. Sess. 1996) (remarks of Representative Saxl) (stating that "49 other states in this country saw fit to adopt legislation which would identify stalking as a crime"). Notably, the Office of the Maine Attorney General disputed the characterization that Maine was the last state in the country to criminalize stalking, apparently believing that Maine's anti-terrorizing statute or its laws regarding protective orders encompassed the criminal offense. *See* Renee Ordway, *Legislator pushing bill on stalking*, BANGOR DAILY NEWS (Jan. 10, 1996), https://archive.bdnblogs.com/1996/01/10/legislator-pushing-bill-on-stalking-act-would-become-crime/ [https://perma.cc/43BH-WFAA].

84. *See* Nat'l Crim. Just. Ass'n, PROJECT TO DEVELOP A MODEL ANTI-STALKING CODE FOR STATES, NAT'L INST. OF JUST. (Oct. 1993).

85. Me. P.L. 1995, ch. 668, § 3 (codified as amended at 17-A M.R.S.A. § 210-A).

86. *Id.*

Representative Saxl, shows that the legislature was particularly concerned with how advances in computer technologies would facilitate stalking. Saxl remarked that the anti-stalking legislation would "make it a crime to invade the lives of victims via computer; by using computer mail or other computer-aided ways to invade a person's bank records, credit card statements and the like, and then using that type of information in the harassment of the individual."[87] He also noted that such problems "have occurred in Maine already," and he anticipated the problem would worsen with "increased computer access."[88]

The legislature would return to the anti-stalking law twice during this era of reform. Both times, the legislature amended the law to account for the use of new technologies to stalk victims in Maine. The 2001 Act to Prohibit Cyberstalking clarified that Maine's stalking law prohibited the conveyance of oral or written threats by "electronic means."[89] Then, as part of a larger legislative effort to strengthen the state's anti-stalking law in 2007-2008, the legislature redefined "course of conduct" to include "2 or more acts, including but not limited to acts in which the actor, by any action, method, device or means, directly or indirectly follows, monitors, tracks, observes, surveils, threatens, harasses or communicates to or about a person or interferes with a person's property."[90] The bill also included a legislative intent section to explain that the revisions were:

> drafted broadly to capture all stalking activity, including a stalker's use of new technologies. Presently, some stalkers use Global Positioning Satellite technology to monitor actions, disposable cell phones to make untraceable calls and keyloggers to capture private information from computers. In the future, new technologies not currently imagined will be used to the same ends. The Legislature intends that the use of such new technology be covered by this legislation.[91]

Maine also revised its Criminal Invasion of Privacy law to account for changes in technology during this time. In 1996, police arrested a Lisbon man who had surreptitiously taken up-skirt videos of women and girls at a bookstore and in other public places.[92] The man had jerry-rigged a briefcase to camouflage a small video camera, which he would place on the ground near where his victims were standing.[93] The incident posed a problem for prosecutors: the criminal invasion of privacy statute only applied to "private places" and the man's conduct did not fit into any other crime enumerated by the state's criminal code.[94] While the man was eventually convicted for criminal invasion of privacy after the judge stretched the statute to

87. Ordway, *supra* note 83.

88. *Id.*

89. Me. P.L. 2001, ch, 411, § 1.

90. Me. P.L. 2007, ch. 685, § 1.

91. *Id.*

92. *See* Robert George, *Bill Targets High-tech Lewdness*, BRUNSWICK TIMES REC. 2 (Feb. 2, 1997), *available from* Me. State Law & Leg. Reference Library by requesting 118/LD00xx/nc118-LD0036/SB118640.pdf.

93. *Id.*

94. *See An Act to Criminalize Unpermitted Visual Surveillance under the Clothing of a Person in a Public Place by Mechanical or Electronic Equipment: Hearing on L.D. 0036 Before J. Standing Comm. on Criminal Justice*, 118th Legis. 9-10 (1997) (letter from Assistant Dist. Att. Carlos Diaz to victim's mother), *available from* Me. State Law & Leg. Reference Library by requesting cf118-LD-036.pdf.

reach his conduct,[95] the legislature was concerned that the case revealed a gap in the criminal code caused by the advance in video-recording technology. The state thus added a new clause to its criminal invasion of privacy statute, making it a crime to engage:

> in visual surveillance in a public place by means of mechanical or electronic equipment with the intent to observe or photograph, or record, amplify or broadcast an image of any portion of the body of another person present in that place when that portion of the body is in fact concealed from public view under clothing and a reasonable person would expect it to be safe from surveillance.[96]

The legislature would amend the criminal invasion of privacy statute twice more during this era to provide additional privacy protections to Mainers. First, increased use of surveillance cameras in retail establishments prompted the legislature to specify that "private place" as defined by the statute included "changing or dressing rooms, bathrooms and similar places."[97] Second, the legislature removed the exception for places "to which the public or a substantial group has access" from the definition of "private place," such that a criminal invasion of privacy could occur by conducting surveillance on someone while they are in a publicly accessible area, provided that they had a reasonable expectation of privacy in that area.[98]

To give its internet-era stalking and invasion of privacy reforms more teeth, Maine added both crimes to the list of offenses that allow a victim to obtain a Harassment Prevention Order.[99] Maine's Protection from Harassment statute, 5 M.R.S.A. §§ 4651-61, allows victims of harassment to obtain emergency protective orders. The term "harassment" is defined to encompass several specific offenses—which now include stalking and criminal invasion of privacy. The statute specifies that a victim can obtain the order "in the District Court of the division in which either the plaintiff or the defendant resides," giving victims recourse when their harasser resides outside of the state and torments them through the internet.[100]

Beyond reforms to protect new intrusions on physical privacy made possible by advances in computing and other technologies, Maine took several measures to protect its residents' information privacy from new and emerging threats. In 2005, a data broker[101] called ChoicePoint experienced a security breach that exposed thousands of consumers' personal information, including approximately 250

---

95. *Id.*

96. Me. P.L. 1997, ch. 467, § 1. The legislature also provided an affirmative defense to this new crime for situations where the person was over 14 years old and consented to the surveillance. The legislative materials that I have reviewed do not reveal why the legislature chose 14 years old as the pertinent age of consent for this incredibly intrusive conduct, but that provision remains the law today. 17-A M.R.S.A. § 511(1-A) (2016).

97. Me. P.L. 1999, ch. 116, § 1.

98. Me. P.L. 2007, ch. 688, § 2 (amending the definition of "private place" as follows: "As used in this section, "private place" means a place where one may reasonably expect to be safe from surveillance, including, but not limited to, changing or dressing rooms, bathrooms and similar places, but excluding a place to which the public or a substantial group has access.").

99. Me. P.L. 2001, ch. 134, § 1.

100. *See* 5 M.R.S.A. § 4652 (2004).

101. For more information on data brokers, see *infra* Section III(B) (proposing that Maine regulate data brokers by creating a data broker registry and giving consumers greater control over how data brokers use their personal information).

Mainers.[102] This event drew the legislature's attention to the growing problem of data breaches and the risk of identity theft that results.[103] The legislature responded to the incident by enacting a breach-notification law: "An Act To Protect Maine Citizens from Identity Theft."[104] The Act applied only to "information brokers"—companies that collected consumers' personal information and then furnished that information to third parties—and required such companies to notify Maine consumers upon discovery of a data breach involving their personal information.[105] Violations of the Act were subject to civil penalties that could be enforced by the Department of Professional and Financial Regulation ("DPFR") or by the Attorney General.[106] The Act also required the DPFR to issue a report on data security and security breaches to inform future changes to the Act.[107]

The DPFR's report contained two key recommendations. First, the report advised that the Act be expanded to apply to all businesses (and certain other persons)—not just information brokers.[108] Second, the report recommended establishing a "limited private cause of action" for actual damages caused by the failure to investigate or timely notify consumers of a breach.[109] Maine swiftly amended the breach notification law to adopt the former recommendation, but the provision creating a limited private cause of action was removed in committee.[110] To this day, there is no private action for violations of Maine's breach notification law.[111]

---

102. *See* ME. DEP'T OF PRO. & FIN. REGUL, REP. OF THE DEP'T OF PRO. & FIN. REGUL. TO THE JOINT STANDING COMM. ON INS. AND FIN. SERVS. ON P.L. 2005, CH. 379 "AN ACT TO PROTECT MAINE CITIZENS FROM IDENTITY THEFT" 1 (2006), http://lldc.mainelegislature.org/Open/Meta/LegHist/122/lh122-LD-1671.pdf [https://perma.cc/U4UW-UXZ4] [hereinafter ME. DEP'T OF PRO. & FIN. REGUL. REP.].

103. *Id.*

104. Me. P.L. 2005, ch. 379.

105. *Id.* § 1.

106. *Id.*

107. *Id.*

108. *See* ME. DEP'T OF PRO. & FIN. REGUL. REP., *supra* note 102, at 6, 12. The report also recommended that the state maintain more stringent notification requirements for information brokers. *Id.* at 12. The State adopted that recommendation by requiring information brokers to provide notice following a breach where a consumer's "personal information has been, or is reasonably believed to have been, acquired by an unauthorized person," while subjecting other businesses to the ostensibly lower standard of having to provide notice only when "misuse" of the personal information has occurred or is "reasonably possible" to occur. 10 M.R.S.A. § 1348(1)(A)-(B). This distinction was likely more imaginary than real, as misuse is almost always "reasonably possible" when an unauthorized personal acquires a person's personal information.

109. ME. DEP'T OF PRO. & FIN. REGUL. REP., *supra* note 102, at 12.

110. L.D. 2017, § 12 (122d Legis. 2006) (codified at 10 M.R.S.A. § 1350) (proposing a private right of action). The legislature subsequently made minor revisions to strengthen its breach notification law in 2007, 2009, and 2019. *See* Me. P.L. 2009, ch. 634, § 1 (codified at 10 M.R.S.A. § 1350-B) (requiring law enforcement to issue police reports to persons whose personal information may have been misused in a data breach); Me. P.L 2009, ch. 161, § 1 (codified at 10 M.R.S.A. § 1347(1)) (expanding the definition of a security breach); Me. P.L. 2019, ch. 512, § 1 (codified at 10 M.R.S.A. § 1347(5)) (applying the law to municipalities and school administrative units).

111. *See* 10 M.R.S.A. §§ 1346-1350-B (2006); *see also In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 125 (D. Me. 2009) (noting that Maine's breach notification statute "does not recognize any private recovery."). The State's efforts to protect its residents from the threat of identity theft posed by new computer technologies continued in 2007, when the legislature enacted "An Act to Help Prevent Identity Theft." Me. P.L. 2007, ch. 626 (codified at 33 M.R.S.A.

Maine also took aim at the unauthorized sale of residents' cell phone information during this era. By 2005, some data brokers were acquiring and offering for sale records of calls made to and from consumers' cell phones. Maine law already prohibited the sale of such records for landlines, but as Maine State Senator Bartlett remarked on the Senate floor, "technology got a couple of steps ahead of us."[112] The legislature thus passed the "Cellular Telephone Customer Privacy Act" to provide civil and criminal penalties for selling, disclosing, or offering to sell or disclose call records and other cell-phone information.[113]

Maine proved to be ahead of the curve on this issue. In 2006, the U.S. House of Representatives Committee on Energy and Commerce began investigating the "activities of Internet-based data brokers who use lies, fraud, and deception to procure . . . customer proprietary network information (CPNI) that is compiled by cell phone carriers."[114] The Committee soon learned that investigators hired by the Hewlett Packard Company ("HP") to look into a boardroom leak used a data broker to obtain cell phone call records of board members and reporters.[115] This revelation, and the Committee's broader investigation into data brokers' practices, led to three Committee hearings on data brokers' collection of personal information,[116] criminal charges against HP's chairwoman (which were eventually dropped),[117] and a $14.5 million settlement with the State of California.[118] The incident also led the federal government to enact the Telephone Records and Privacy Protection Act of 2006, prohibiting the fraudulent access of phone records and the unauthorized sale of such records.[119]

The end of this era of privacy reform in Maine can be marked by two 2011 bills designed to update Maine's laws to account for the increased use of computers in harassment. First, Maine's 1975 law on annoying telephone calls, discussed *supra* Section I(A), was badly in need of updating because, by the 2000s, harassing calls were often placed from computers and not telephones. The legislature thus amended section 506 of the criminal code to cover harassment "by electronic communication device," which it defined to include "any software capable of sending and receiving communication."[120] Second, the national—and indeed global—nature of internet privacy intrusions led the state to amend its criminal invasion of computer privacy

---

§651-B). This sensible piece of legislation allowed individuals to request that certain personal information (social security numbers, driver's license numbers, financial account numbers, and the like) be redacted from records accessible through a registry of deeds website. *Id.* § 1.

112. Legis. Rec. S-1831 (2d Reg. Sess. 2006) (remarks of Sen. Bartlett).

113. Me. P.L. 2005, ch. 582.

114. Letter from Comm. on Energy & Com., to Patricia Dunn, Chairwoman of the Bd. of Hewlett-Packard Co. 1 (Sept. 11, 2006), https://web.archive.org/web/20061107225224/http://i.n.com.com/pdf/ne/2006/househp_letter.pdf.

115. *Id.* at 1-2.

116. *Internet Data Brokers: Who Has Access to Your Private Records?: Hearings Before the Subcomm. on Oversight & Investigations of the Comm. on Energy & Com. H.R.*, 109th Cong. (2006).

117. Rob Kelley, *Charges Against HP's Dunn Dropped*, CNN MONEY (Mar. 14, 2007, 7:51 PM), https://money.cnn.com/2007/03/14/technology/hpq/index.htm [https://perma.cc/TG4N-SX76].

118. Scott Horsley, *HP to Pay $14.5 Million to Calif. In 'Pretexting' Case*, NPR (Dec. 8, 2006, 6:00 AM), https://www.npr.org/templates/story/story.php?storyId=6597192 [https://perma.cc/2KYS-T5P6].

119. Telephone Records and Privacy Protection Act of 2006, Pub. L. 109-476, § 3, 120 Stat. 3568, 3569.

120. Me. P.L. 2011, ch. 464, § 14.

crimes to specify that the state had jurisdiction to prosecute persons who committed such crimes when they were physically located outside of the state, so long as the victim was a Maine resident.[121]

***

By 2011, Maine had updated its existing laws and implemented new laws to account for some of the privacy intrusions created or exacerbated by the large-scale adoption of computers and the internet. However, there was much left unaddressed by this era of reform. Social media, big data, machine learning, and other new technologies were emerging and expanding rapidly. These new developments would pose privacy threats that Maine's internet-era reforms were ill-equipped to remediate.

C. Reforms for the Era of Social Media, Big Data, and Machine Learning

From the early 2010s through present day, we have been living in an era where the threats to individual privacies posed by technological advances are complex, systemic, and rapidly evolving. While much has been written about these privacy risks, Shoshana Zuboff's *The Age of Surveillance Capitalism* is perhaps the leading account of the era.[122] Zuboff describes the business models employed by participants in what she calls the "surveillance economy."[123] Companies ranging from social media platforms, to search engines, to manufacturers of "internet of things" ("IoT") devices provide services and products that collect massive amounts of data about their users.[124] This data serves as the "raw material[]" for machine-learning "prediction products" that are designed to "forecast what we feel, think, and do: now, soon, and later."[125] Surveillance capitalists then sell these prediction products to advertisers who use the products to target their advertisements to the users who are most likely to purchase their goods or services.[126]

The success of this economic model hinges on being able to accurately predict, and indeed to positively shape, how users will behave.[127] Improving accuracy, in turn, requires obtaining more and more data to feed the increasingly complex

---

121. Me. P.L. 2011, ch. 377, § 1. The state also amended the jurisdictional provisions of the computer crimes law to specify that a prosecution could occur in the county where the defendant accessed the computer resource or in the country in which the affected computer resource was located. Me. P.L. 2011, ch. 133, § 1.

122. *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 94 (2019).

123. *Id.*

124. *See id.* at 93-95 (describing how Google and other surveillance capitalists collect and monetize users' personal information).

125. *Id.* at 94-96.

126. *Id.* at 96. While advertisers are currently the primary customers in the surveillance capitalist marketplace, Zuboff explains that there is no reason to expect that the market will remain limited to that group. "The new prediction systems are only incidentally about ads . . . . [A]ny actor with an interest in purchasing probabilistic information about our behavior and/or influencing future behavior" is a potential customer. *Id.* at 96-97.

127. *See id.* at 95 (explaining that even slight increases in the accuracy of predicting behaviors can yield substantial increases in profits); *id.* at 293 (describing how surveillance capitalists have begun to progress from predicting user behavior to modifying user behavior).

machine-learning algorithms that inform prediction products.[128] Thus, the more data about people a product can collect, the more lucrative that product may be for its creator.

The privacy threats arising from an economic model dependent on collecting ever-increasing amounts of personal information are significant. The model results in an intrusive "hunt" for personal information, during which no facet of human existence is off limits.[129] Surveillance capitalists thus aim to collect data about us when we browse the internet, watch television, play music, exercise, sleep, drive our cars, heat our homes, and when we partake in virtually every other facet of society. The decisions driven by companies' use of this information may be innocuous (Which cat photo should we show this person?), life-altering (Should we insure this person?), or may pose systemic implications for democracy that we are still coming to understand (Which candidate is this person likely to support?).

Additionally, the large amounts of information made available to surveillance capitalists leave consumers vulnerable to the exploits of third parties. People can be hacked, brigaded, doxed, bullied, humiliated, or impersonated on social media, creating severe consequences for privacy, identity, and safety in the "real world." New technologies like facial recognition, biometric trackers (such as a FitBit), drones, and advances in genetic testing have created thousands of new data points that can similarly be used and exploited by companies, governments, and third parties. And the volume and nature of the personal information that surveillance capitalists store exacerbates the existing harm caused by data breaches—a problem that is certain to further accelerate as we become increasingly dependent on the internet for goods and services as a result of the COVID-19 crisis.

Like many states, Maine is still very much in the process of grasping the scope of these privacy challenges and crafting appropriate legislative responses to them. Thus far, Maine has enacted targeted reforms designed to combat specific problems posed by the technological advances of this era. The state has acted to protect victims of cyberharassment, to guard employees' social media accounts from employers, to protect the privacy of K-12 students from education technology providers, to regulate the use of drones by law enforcement, and to establish consumer privacy protections that apply to internet service providers ("ISPs").

As in the two previous eras discussed above, Maine began this era of reform by protecting the residents who are perhaps most vulnerable to online privacy intrusions: victims of harassment. The ubiquity of smartphones and smartphone cameras has led to two particularly disturbing forms of privacy intrusion that are most commonly suffered by young women. The first occurs when a person sends a victim an unauthorized and unsolicited sexual image. The victim in such situations usually has no opportunity to avoid seeing the image: when they open the text message, social media message, or email, the image is instantly before them.

---

128. *See, e.g.*, *id.* at 95 ("Google's machine intelligence capabilities feed on behavioral surplus, and the more surplus they consume, the more accurate the prediction products that result.").

129. *See, e.g.*, *id.* at 93-94 (describing how surveillance capitalists once "found" personal information by analyzing users' online behavior, but how personal information is now "hunted aggressively and produced largely through surveillance"); *id.* at 497 (describing surveillance capitalists' goals of obtaining "total information" in order to produce "certainty and the promise of guaranteed outcomes" for their prediction products).

The legislature decided to address this form of lewd behavior by adding a new offense to section 506 of the criminal code: "Harassment by telephone or electronic communication device."[130] The new provision makes it a Class D crime to "send[] an image or video of a sexual act . . . or of the actor's or another person's genitals" with "intent to cause affront or alarm or for the purpose of arousing or gratifying sexual desire," to: (1) a minor under 14 years old; (2) a minor age 14 or 15, if the offender is at least 5 years older than the minor; or (3) a person with a mental disability that was reasonably apparent to the offender.[131] The provision makes it a Class E crime to send such an image or video without consent when the person receiving the image or video has notified the actor that they do not consent to receive the images or videos.[132]

The second intrusion occurs when a person posts nude images of another person online without their consent. This is known as "revenge porn," as it typically occurs when a couple breaks up and one of the individuals posts the photos of their ex.[133] Images may be posted on social media, on a general porn site, or on sites specifically dedicated to hosting revenge porn.[134] The victims are almost always women.[135] Testimony from the Director of Public Policy of the Maine Women's Lobby before the Committee on Criminal Justice and Public Safety succinctly summarizes the problem:

> One of the ways in which our laws have failed to protect victims of abuse is non-consensual pornography or "revenge porn". In some cases, intimate recordings or photos may be taken consensually during a positive time in a relationship to be kept private between intimate partners. But, sometimes, these recordings or images may be taken non-consensually, either without the victim's knowledge or under duress, as part of a larger pattern of control and abuse. Later, these images are secretly uploaded to a website created for this very purpose. . . . [T]his horrifying act is made even worse when the pictures are accompanied by identifying information, potentially including a name, a town, or even a physical address of the victim's home or place of employment. Some sites seek to profit from the posting of these images, demanding thousands of dollars to have the image removed from each website to which it was shared.[136]

---

130. Me. P.L. 2017, ch. 397 § 1.

131. *Id.*

132. *Id.* (codified at 17-A M.R.S.A. § 506(1)(A-2)).

133. *See* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 17 (2014) (defining "revenge porn" as "the posting of individuals' nude photographs without their consent"). For additional materials on revenge porn, *see generally* Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345 (2014); Zak Franklin, Comment, *Justice for Revenge Porn Victims: Legal Theories to Overcome Claims of Civil Immunity by Operators of Revenge Porn Websites*, 102 CALIF. L. REV. 1303 (2014); Jenna K. Stokes, Note, *The Indecent Internet: Resisting Unwarranted Internet Exceptionalism in Combating Revenge Porn*, 29 BERKELEY TECH. L.J. 929 (2014).

134. *See, e.g.*, CITRON , *supra* note 133, at 45-46 (telling the story of a revenge porn victim whose sexual images and contact information were shared on a site dedicated to revenge porn, on social media, and on other websites).

135. *Id.* at 17 (stating that "most often, revenge porn features women" and citing a study showing that 90 percent of revenge porn victims were female).

136. *An Act to Prohibit the Unauthorized Dissemination of Certain Images: Hearing on L.D. 679 Before the Me. J. Comm. on Crim. Justice and Pub. Safety*, 127th Legis. 23 (2015) (testimony of Danna

The Committee heard more testimony regarding the impact revenge porn had on Maine residents when it considered L.D. 679, "An Act to Prohibit the Unauthorized Dissemination of Certain Private Images."[137] For example, Representative Grant shared a story of a Maine woman whose partner filmed her "without her knowledge having relations," and then "threatened to put [the] images on the Internet unless she submitted to his demands."[138] Representative Russell highlighted a similar story from the *Bangor Daily News* which focused on a woman whose abusive ex created a fake Facebook page with her identifying information, nude images, and a link to a website with images of her performing sexual acts and encouraging people to contact her for sex.[139] Pine Tree Legal provided testimony showing that forty-four requests for protection from abuse orders or harassment in Portland District Court involved revenge porn in 2014.[140]

L.D. 679 passed through the legislature and went into effect on October 15, 2015, adding Maine to the list of approximately twenty-one other states that had criminalized revenge porn.[141] With some exceptions, the Act made it a crime when a person "knowingly disseminates, displays or publishes. . . with intent to harass, torment, or threaten," a photograph, videotape, film or digital recording of another person in a state of nudity or engaged in a sexual act . . . when the person knows or should have known that the depicted person" is age 18 or older, is identifiable, and has not consented.[142] The Act also gave victims the ability to obtain an protection from abuse order in Maine district court.[143]

During the same legislative session in which Maine enacted its revenge porn law, the state also established a key privacy protection for employees who use social media platforms. A social media account holds a tremendous amount of personal information. The account holder may make some of this information public, in which case it can be viewed by anyone with internet access, including an employer or prospective employer. But other information may be private. Social media users

---

Hayes, Director of Public Policy, Maine Women's Lobby), *available from* Me. State Law & Leg. Reference Library by requesting cf123-LD-0679.pdf.

137. L.D. 679 (127th Legis. 2015) (originally enacted by Me. P. L. 2015, ch. 339, § 1).

138. *An Act to Prohibit the Unauthorized Dissemination of Certain Images: Hearing on L.D. 679 Before the Me. J. Comm. on Crim. Justice and Pub. Safety*, 127th Legis. 23 (2015) (testimony of Rep. Gay M. Grant).

139. *Id.* at 11-13 (testimony of Rep. Diane Russell); *see also* Regina Rooney, *The Abuse Follows Her Everywhere, and it's Legal: One Woman's Story of Revenge Porn*, BANGOR DAILY NEWS (Apr. 20, 2015), https://bangordailynews.com/2015/04/20/mainefocus/the-abuse-followed-her-everywhere-one-womans-story-of-revenge-porn/ [https://perma.cc/ DC5C-BZPA].

140. *An Act to Prohibit the Unauthorized Dissemination of Certain Images: Hearing on L.D. 679 Before the Me. J. Comm. on Crim. Justice and Pub. Safety*, 127th Legis. 23 (2015) (testimony of Lucia Chomeau Hunt).

141. *See* END REVENGE PORN, *Frequently Asked Questions*, https://web.archive.org/web/20151017065602/http://www.endrevengeporn.org/faqs (archived on Oct. 17, 2015) (listing 21 states that had enacted revenge porn laws as of July 2015). Today, 46 states and the District of Columbia have passed criminal laws regarding revenge porn. *46 States + DC + One Territory Now Have Revenge Porn Laws*, CYBER C.R. INITIATIVE, https://www.cybercivilrights.org/revenge-porn-laws/ [https://perma.cc/8A5M-V477] (last visited Apr. 27, 2021).

142. Me. P.L. 2015, ch. 339, § 1.

143. *Id.* The legislature would soon amend the Act to ensure that images and identifying information filed in revenge porn proceedings were kept under seal and to more fully integrate the Act with the state's abuse—and harassment—prevention laws. *See* Me. P.L. 2015, ch. 410.

can adjust their privacy settings such that their content can be viewed only by their "friends" or "followers" and platforms allow users to privately message each other.

In response to reports of employers and educational institutions requiring employees or students to provide the employer or institution access to their social media accounts, state lawmakers around the country began proposing legislation to ban that practice.[144] By the end of 2012, six states had enacted legislation protecting employees or students from these intrusive demands.[145] Maine joined this trend in 2015 by prohibiting employers and prospective employers from requiring an employee or applicant to disclose their social media passwords, access their accounts in the employer's presence, provide information about their accounts, disclose contacts associated with their accounts, adjust the privacy settings of their accounts, discipline employees for failing to comply with such requests, or decline to hire an applicant for failing to comply with such requests.[146]

Maine also created privacy protections for students during this time by enacting the "Student Information Privacy Act" ("SIPA").[147] The SIPA regulates "operators," which are entities that: (a) operate a website, online service, or application with "actual knowledge" that the website, service or application is used for K-12 school purposes "and was designed and marketed" for K-12 school purposes; and (b) collect, maintain, or use student personal information in a digital or electronic format.[148] The SIPA subjects operators to several restrictions on how they can use and disclose students' data. Most notably, operators may not use student data to engage in targeted advertising or to amass a profile about a student, sell student data, or disclose student data to third parties (with some exceptions for service providers, government agencies, and the like).[149] Operators must maintain reasonable security procedures and practices.[150] And, operators must delete student data within forty-five days of receiving a request to delete from a school.[151]

While the reforms of this era focused primarily on the privacy abuses attendant to new technologies when they are in the hands of private actors, such technologies may also be used and abused by governments. In 2015, Maine enacted a law

144. *See* Samuel A. Thumma, *When You Cannot "Just Say No": Protecting the Online Privacy of Employees and Students*, 69 S.C. L. REV. 1, 3 (2017) (noting the "reported incidents where employers and educational institutions have demanded, and received" access to social media accounts); *id.* at 9-27 (reviewing different state legislative approaches to regulating employers' and educational institutions' access to their employees' or students' social media accounts).

145. *See id.* at 9-10 ("Six states enacted [social media access] legislation in 2012, with Maryland and Illinois enacting laws in the employment context, Delaware and New Jersey enacting laws in the educational context, and California and Michigan enacting laws in both the employment and educational contexts."). For a complete list of all bills proposed by state lawmakers pertaining to social media account access, *see Employer Access to Social Media Usernames and Passwords*, NAT'L CONF. OF STATE LEGISLATURES, https://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx [https://perma.cc/2QHK-UULT] (last visited Nov. 17, 2020) (compiled by the National Conference of State Legislatures).

146. Me. P.L. 2015, ch. 343, § B-1. The law does contain a notable exception for investigations into misconduct in which the employer "reasonably believes" social media information may be relevant. *Id.*

147. Me. P.L. 2015, ch. 256.

148. *Id.* (codified as amended at 20-A M.R.S.A. § 952(4)).

149. *Id.* (codified as amended at 20-A M.R.S.A. § 953).

150. *Id.*

151. *Id.*

designed to curtail government abuses of one new technology that has enjoyed widespread adoption during this era: drones. Drones are unmanned aerial vehicles that may be equipped with surveillance technologies.[152] They have numerous uses, which may be innocuous (scenic photography),[153] highly beneficial (facilitating search and rescue operations),[154] financially lucrative (automated delivery of packages),[155] dangerously abusive (stalking),[156] or downright dystopian (mass surveillance of citizens).[157]

In the hands of law enforcement, drones could be used to "engage in constant, blanket surveillance of people," particularly given the "decreasing cost and increasing capabilities" of drones over the last several years.[158] Maine's "Act to Protect the Privacy of Citizens from Domestic Unmanned Aerial Vehicles" guards against these potential abuses by creating a regulatory framework for law enforcement's use of drones.[159] First, the Act requires prior approval from "the

---

152. *See, e.g.*, Hillary B. Farber, *Eyes in the Sky: Constitutional and Regulatory Approaches to Domestic Drone Deployment*, 64 SYRACUSE L. REV. 1, 8 (2014) (describing drones and their advantages for use in surveillance); *see also* DJI, Mavic Air 2 Specifications, https://www.dji.com/mavic-air-2/specs [https://perma.cc/63R3-NU7D] (last visited Nov. 17, 2020) (detailing the capabilities of a mass-marketed drone, including its camera technology).

153. *See* Michael L. Smith, *Regulating Law Enforcement's Use of Drones: The Need for State Legislation*, 52 HARV. J. ON LEGIS. 423, 423 (2015) (noting that private actors "use drones for hobbyist purposes").

154. *See* Department of Homeland Security, *Snapshot: First Responders Assess Drones for Search and Rescue Missions*, (Apr. 2, 2020) https://www.dhs.gov/science-and-technology/news/2020/04/02/snapshot-first-responders-assess-drones-search-and-rescue-missions [https://perma.cc/7PEN-V95B] (describing the various ways in which first responders can use drones and stating that "[s]mall drones offer tremendous potential for emergency response missions").

155. *See, e.g.*, *Amazon Unveils Futuristic Plan: Delivery by Drone*, CBS NEWS (Dec. 1, 2013), http://www.cbsnews.com/news/amazon-unveils-futuristic-plan-delivery-by-drone/ [https://perma.cc/8623-QWTJ] (announcing Amazon's plans to use drones to deliver merchandise); Jeff Wilke, *A Drone Program Taking Flight*, AMAZON (June 5, 2019), https://www.aboutamazon.com/news/transportation/a-drone-program-taking-flight [https://perma.cc/3TED-JW2J] (unveiling an Amazon Prime air drone "that can fly up to 15 miles and deliver packages under five pounds to customers in less than 30 minutes"). *See generally* Steve Calandrillo et al., *Deadly Drones? Why FAA Regulations Miss the Mark on Drone Safety*, 23 STAN. TECH. L. REV. 182 (2020) (critiquing the Federal Aviation Administration's approach to regulating drones).

156. *See* Petition from Electronic Privacy Information Center (EPIC) to the Fed. Aviation Admin. 3 (Feb. 24, 2012), https://epic.org/apa/lawsuit/EPIC-FAA-Drone-Petition-March-8-2012.pdf [https://perma.cc/P86C-HGGP] (raising the possibility that "[c]riminals and other may use drones for purposes of stalking and harassment").

157. *See, e.g.*, Mark Hanrahan, *Coronavirus: China Deploys Drones with Cameras, Loudhailers to Chastise People for Unsafe Behavior*, ABC NEWS (Feb. 4, 2020, 9:46 AM), https://abcnews.go.com/International/coronavirus-china-deploys-drones-cameras-loudhailers-chastise-people/story?id=68746989 [https://perma.cc/56YC-3VHT] (describing how China has used drones to enforce social distancing rules during the coronavirus pandemic).

158. Smith, *supra* note 153, at 440-41; *see also* Farber, *supra* note 152, at 2 ("State and local police departments are eager to equip themselves with drones because they are cheaper and more efficient than helicopters and other types of manned aircraft.").

159. Me. P.L. 2015, ch. 307 (codified at 25 M.R.S.A. § 4501). In the legislative findings section of the Act, the legislature noted several potential benefits to drones, but concluded that "the technology also presents a potential threat to the privacy of citizens of this State if used by law enforcement in the conduct of criminal investigations without appropriate guidelines and supervision." *Id.* (codified at 25 M.R.S.A. § 4501(1)).

governing body of the governmental unit overseeing the law enforcement agency" before the agency can acquire a drone.[160] Second, the Act limits how drones may be used. Most significantly, law enforcement agencies must obtain a warrant to use a drone, unless the drone's use would be permitted by an exception to the warrant requirement under the U.S. Constitution or the Constitution of Maine.[161] They are prohibited from using weaponized drones and from using drones to surveil peaceful protests, but they may use drones for non-investigatory purposes, such as search and rescue operations or assessing damage caused by natural disasters.[162] Third, the Act requires the Trustees of the Maine Criminal Justice Academy to develop minimum standards governing the use of drones by law enforcement agencies. The standards must include training requirements; requirements to obtain prior approval from higher-ups prior to use; restrictions on the use of intrusive technologies such as high-powered zoom lenses, video analytics, thermal imaging, and facial recognition; procedures to minimize intrusions on third parties who are not the subject of an investigation; and more.[163] Finally, the Act contains a transparency requirement pursuant to which the Commissioner of Public Safety must compile summaries of law enforcement agencies' drone use and warrant requests for deploying drones.[164]

Most recently, Maine became the first (and thus far the only) state in the nation to regulate ISPs' use of their customers' personal information. Maine passed "An Act to Protect the Privacy of Online Customer Information" shortly after the Trump Administration nixed the Federal Communication Commission's attempt to regulate the same.[165] The Act requires ISPs to obtain consumers' consent before using, disclosing, or selling their personal information; to take reasonable security measures to protect consumers' personal information; and to provide consumers notice of their rights and the ISPs' obligations under the Act.[166]

---

160. *Id.* (codified at 25 M.R.S.A. § 4501(3)).

161. *Id.* (codified at 25 M.R.S.A. § 4501(4)(B)).

162. *Id.* (codified at 25 M.R.S.A. § 4501(4)(C)-(F)).

163. *Id.* (codified at 25 M.R.S.A. § 4501(5)). The Act also contains an exception whereby lay enforcement agencies can use drones without adopting these standards in emergency situations, with approval from the agency's chief or the Governor. *See id.* (codified at 25 M.R.S.A. § 4501(4)(G)).

164. *Id.* (codified at 25 M.R.S.A. § 4501(6)). For a comparative evaluation of how other states have regulated law enforcement's use of drones, *see* Smith, *supra* note 153, at 427-39 (comparing legislation from Florida, Idaho, Illinois, Indiana, Iowa, Montana, North Carolina, Oregon, Tennessee, Texas, Utah, Virginia, and Wisconsin).

165. Me. P.L. 2019, ch. 216; *see also* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rec. 13911 (2017); David Shepardson, *Trump Signs Repeal of U.S. Broadband Privacy Rules*, REUTERS (Apr. 3, 2017, 7:50 PM), https://www.reuters.com/article/us-usa-internet-trump/trump-signs-repeal-of-u-s-broadband-privacy-rules-idUSKBN1752PR [https://perma.cc/5BF7-G4P4].

166. Me. P.L. 2019, ch. 216. There is good reason for targeting ISPs for additional regulation when it comes to consumer privacy protections. ISPs have access to information regarding every website a user visits and have at times used this access "in privacy-invasive ways, like creating extensive portfolios of their users' online activity and injecting 'super cookies' that allow third parties to track individual customers." Arianna Demas, *Maine's ISP Privacy Law Does Not Violate the First Amendment, Much as ISPs Would Like for It To*, ACLU (May 29, 2020), https://www.aclu.org/news/privacy-technology/maines-isp-privacy-law-does-not-violate-the-first-amendment-much-as-isps-would-like-for-it-to/ [https://perma.cc/BF76-5FYT]. And, as the bill's sponsor put it, interacting with an ISP is "not optional" like visiting a particular website or using a particular software may be; the internet is increasingly a necessity. Steve Mistler, *Maine Lawmakers Send One Of The Country's Toughest*

The state's early-mover status drew the ire of industry groups, who promptly filed suit in federal district court in Bangor. The complaint in *ACA Connects v. Frey* argues that the Maine law violates the First Amendment guarantee of free speech by, *inter alia*, requiring ISPs to obtain consent before using customers' personal information.[167] The complaint also argues that the statute's "amorphous, broad, and open-ended restrictions will . . . [unconstitutionally] chill ISPs' protected First Amendment speech."[168] The case has received national attention, including an amicus brief in support of the Act jointly filed by the ACLU, the Electronic Frontier Foundation, and the Center for Democracy and Technology.[169] As of this writing, the district court has denied the plaintiffs' motion for judgment on the pleadings—rejecting their First Amendment arguments at that stage of the proceedings—and the matter is continuing through the discovery stage of litigation.[170]

D. Summary of Maine Privacy Law

Over the last five decades, Maine has developed a body of privacy law designed to protect against threats to individual privacy that have evolved and expanded with technological advances. These protections include many foundational privacy laws that can be found in most jurisdictions across the country—laws governing wiretapping, credit reporting, unauthorized computer access, stalking and harassment, private investigators, polygraphs, and data breaches are some examples. In more recent years, Maine has risen to the challenge of protecting its residents' privacy by passing modern privacy laws aimed at emerging privacy risks. Such laws include the state's regulation of ISPs, education technology providers, employers' access to social media accounts, and law enforcement's use of drones.

Despite Maine's recent efforts to respond to the new privacy challenges posed by advances in big data, social media, machine learning, and other new technologies, there is much work to be done. Maine's new privacy laws are largely intended to protect *specific* vulnerable segments of the population, regulate *specific* actors, or guard against intrusions posed by *specific* new technologies. This targeted approach to privacy reform cannot account for the myriad privacy threats that Maine residents face today. It does not safeguard Mainers' privacy from the surveillance capitalist economic model discussed above and it leaves residents vulnerable to certain new technologies that carry potential for serious privacy intrusions.

To be sure, this critique could be repeated for nearly every state in the nation as well as the federal government. But Maine can and should do better. In Part III of this Article, I propose several reforms that would fill these gaps and make Maine a national leader in protecting its residents' privacy.

Internet Privacy Proposals To The Governor's Desk, ME. PUB. RADIO (May 3, 2019), https://www.mainepublic.org/post/maine-lawmakers-send-one-countrys-toughest-internet-privacy-proposals-governor-s-desk [https://perma.cc/MTS5-JQG3] (quoting Democratic state Senator Shenna Bellows).

167. *See* Complaint at 2, ACA Connects v. Frey, No. 1:20-cv-00055 (D. Me. Feb. 14, 2020).

168. *Id.* at 4. The complaint also alleges that federal law preempts the Act. *Id.*

169. *See* ACLU et. al as Amici Curiae Supporting Defendant, ACA Connects v. Frey, 471 F. Supp. 3d 318 (D. Me. July 7, 2020).

170. *See ACA Connects*, 471 F. Supp. 3d at 322, 328. The court also rejected the plaintiffs' claim that federal law preempts the Act. *Id.* at 326.

III. MODERNIZING MAINE PRIVACY LAW

In Part III of this Article, I propose two categories of privacy reforms. First, Maine should enact a general consumer privacy statute to give residents control over how companies collect, use, and share their personal information and to protect residents from companies that use their personal information in problematic ways. Section II(A) begins by providing overviews of two possible models for a Maine consumer privacy law—the California Consumer Privacy Act ("CCPA") and the European Union's General Data Protection Regulation ("GDPR"). Drawing from these privacy regimes, I then advance several recommendations to shape a consumer privacy law for Maine. Second, Maine should supplement the general consumer privacy law with new laws aimed at emerging privacy threats that require closer regulation. In Section II(B), I identify five areas in which targeted legislation would be desirable: facial recognition technology; biometric information; smart-home devices; data brokers; and the Maine Information and Analysis Center. I then suggest desirable features of potential legislation for each of these issues.

A. Consumer Privacy Protections

Enacting a general consumer privacy law that gives consumers rights to their personal information and imposes privacy obligations on businesses is perhaps the most significant step Maine can take toward protecting its residents' privacy. Such a law should include the creation of a state agency dedicated to protecting residents' privacy and it should vest that agency with rulemaking authority to address new privacy threats as they emerge and evolve.

There are two existing models on which Maine could pattern a consumer privacy law: the GDPR and the CCPA. Both governing models vest consumers with individual rights to their personal information and impose affirmative obligations on businesses to effectuate those rights and safeguard consumer personal information. However, the scope of individual rights and business obligations created by the two laws differ in important respects and the laws' enforcement mechanisms vary as well. Both privacy regimes are worth examining in fashioning a consumer privacy law for Maine.

1. Potential Templates for a Maine Consumer Privacy Model: The GDPR

The GDPR is regarded as the world's most stringent data privacy regime. The 2016 law regulates how "controllers" (a person that determines the "purposes and means of the processing of personal data") and "processors" (a person who processes personal data on behalf of a controller) collect, use, and share the "personal data" ("any information relating to an identified or identifiable natural person") of "data subjects" (an "identifiable natural person").[171] A complete analysis of the GDPR is beyond the scope of this Article, but providing a basic understanding of data subjects' rights, the obligations imposed on controllers and processors, and the law's

171. Commission Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 4, 2016 O.J. (L 119) (EU) [hereinafter GDPR] ("Definitions").

enforcement mechanisms is important to framing a Maine consumer privacy law.

a. Data Subjects' Individual Rights

Right of Access: Data subjects have the right to access their personal data. The right of access allows the data subject to obtain from a controller who is processing their personal data the purposes of the processing; the types of personal data being processed; the persons to whom personal data may be disclosed; the duration the controller will store the subject's personal information; and more.[172] Data subjects also have the right to know whether the processing of their personal data includes the use of automated decision-making or the use of "profiling," and to obtain certain information about the nature and purpose of such processing.[173]

Right to Data Portability: The right to data portability supplements the right of access to ensure that data subjects can receive a copy of their personal data in a "structured, commonly used and machine-readable format" that allows the subject to transfer the data to another controller (i.e., a competitor) without hinderance.[174]

Right to Rectification: Data subjects have the right to rectify—or correct—inaccurate or incomplete personal information held by a controller.[175]

Right to Erasure: The right to erasure, also known as the right to be forgotten, gives data subjects the right to require controllers to erase their personal data.[176] This right is not absolute. There are several exceptions that would allow a controller to decline to erase a data subject's personal data.[177]

Right to Restriction of Processing: There may be situations in which a data subject contests the controller's processing of their personal data but does not want the controller to erase the contested data. In that and similar situations, the GDPR gives data subjects the right to instruct a controller to restrict processing their personal data. This right requires the controller to stop processing the subject's personal data, but to continuing storing that data instead of erasing it.[178]

Right to Object: Data subjects have the right to object to the processing of their personal information.[179] While this right has some exceptions, a controller must always honor a data subject's objection to the use of their personal data for direct marketing purposes, creating an effective right to "opt-out" from the use of personal data for such purposes.[180]

---

172. *See Id.* art. 15 ("Right of access by the data subject").

173. *Id.* "Profiling" means "any form of automated processing . . . consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements." *Id.* art. 4 ("Definitions").

174. *Id.* art. 20 ("Right to data portability").

175. *Id.* art. 16 ("Right to rectification").

176. *Id*. art. 17 ("Right to erasure ('right to be forgotten')").

177. For example, a controller may decline to erase personal data in some situations where there is an "overriding legitimate ground[]" for the processing, where the processing is necessary "for exercising the right of freedom and expression and information," and for "reasons of public interest in the area of public health." *Id*. art. 17.

178. *Id*. art. 18 ("Right to restriction of processing").

179. *Id.* art. 21 ("Right to object").

180. *Id.* (creating an exception whereby the controller can continue processing personal data if they demonstrate "compelling legitimate grounds for the processing which override the interests, rights and

Automated Processing Rights: Data subjects have the right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal [or similarly significant] effects concerning him or her."[181] As with other GDPR rights, data subjects' automated processing rights are qualified. Controllers and processors may engage in automated decision-making if it is necessary to the performance of a contract with the data subject or if they obtain the data subject's "explicit consent."[182] However, even where these exceptions apply, the controller must take steps to protect the data subject's rights and freedoms, including the right to obtain "human intervention" in the automated decision-making process, and the right for the data subject to contest the automated decision.[183] Moreover, automated decisions may not be based on sensitive characteristics such as race, ethnicity, political opinion, religion, and sexual orientation.[184]

b. Controllers' and Processors' Privacy Obligations

The obligations the GDPR imposes on controllers and processors are designed to effectuate these individual rights. These obligations are extensive and nuanced; only a brief overview is necessary to frame the conversation for proposing a Maine consumer privacy law.

First, controllers must have a legal basis for processing a data subject's personal information. The GDPR enumerates six legal bases for processing, the most commonly invoked of which are processing by consent or processing pursuant to a contract with the data subject.[185] Because most websites use consent as the legal basis for processing personal data obtained through cookies and similar web-tracking tools, companies that are subject to the GDPR (and many who are not) have added "cookie banners" to their websites, which ask users to consent to the collection of personal information before using the website.[186]

Second, the GDPR imposes restrictions on how controllers and processors can collect and process data.[187] Many people have personal data under the control of dozens, if not hundreds, of controllers. Managing how controllers use that data can be a full-time job in and of itself. The GDPR's collection and processing restrictions

---

freedoms of the data subject or for the establishment, exercise or defence of legal claims"); *id.* ("Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.").

181. *Id.* art. 22.

182. *Id.* The right also does not apply if the decision-making is "authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests." *Id.*

183. *Id.*

184. *Id.* There are narrow exceptions that allow automated decision-making on these bases in some situations where the controller has obtained consent or there is a substantial public interest for the processing. *See id.* (referencing the sensitive characteristics and the exceptions contained in GDPR art. 9, "Processing of special categories of personal data").

185. *See id.* art. 6.

186. *See generally* Martin Degeling et al., *We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy*, NETWORK & DISTRIBUTED SYS. SEC. (NDSS) SYMP. 2019 (conducting an examination of 6,579 of the most popular websites in the EU's 28 member states and concluding that by February 2019 62.1% of the websites had added cookie banners).

187. *See* GDPR, *supra* note 171, art. 5 ("Principles relating to processing of personal data").

are designed to shift some of the burden onto controllers for ensuring that personal data is used in accordance with the data subject's expectations. The restrictions include obligations to minimize the amount of personal data a controller or processor uses ("data minimization"), to collect personal data only for specified purposes and to use the data only for those purposes ("purpose limitation"), and to store personal data in an identifiable format for no longer than is necessary for the specified purpose(s) of the processing ("storage limitation").[188] Controllers must operationalize these restrictions by implementing "appropriate technical and organizational measures."[189]

Third, controllers have several notification obligations designed to facilitate data subjects' exercise of their rights.[190] This includes disclosing to the data subject, at the time when personal data is collected, the identity of the controller, the purposes of the processing and the legal basis of the processing, third parties with whom the data may be shared, details about data subjects' rights, any use of automated decision-making, and more.[191] Additionally, upon receipt of a request to delete or to rectify, controllers must notify third parties with whom they have shared the data subject's personal data, such that the data subject does not need to separately submit a request to each person with whom the controller shares their personal data.[192]

Fourth, the GDPR imposes heightened requirements for processing certain sensitive types of personal data. This includes processing children's personal data[193]; processing personal data pertaining to criminal convictions and offenses;[194] processing personal data revealing sensitive demographic information such as race, religion, political opinion, or sexual orientation;[195] and processing genetic data or biometric data.[196]

c. Enforcement

The final aspect of the GDPR that is important to understand in considering a framework for a Maine consumer privacy law is the GDPR's approach to enforcement. The GDPR requires EU member states to vest regulatory authority

---

188. *Id.*

189. *Id.* art. 25 ("Data protection by design and by default").

190. *See id.* art. 12 ("Transparent information, communication and modalities for the exercise of the rights of the data subject").

191. *See id.* art. 13 ("Information to be provided where personal data are collected from the data subject"); *Id.* art. 14 ("Information to be provided where personal data have not been obtained from the data subject").

192. *See id.* art. 19 ("Notification obligation regarding rectification or erasure of personal data or restriction of processing").

193. *See id.* art. 8 ("Conditions applicable to child's consent in relation to information society services") (requiring parental consent for processing personal information of children under age 16).

194. *Id.* art. 10 ("Processing of personal data relating to criminal convictions and offences") (allowing processing of such information only under government control or supervision, unless otherwise authorized by a Union or Member-State law that contains appropriate safeguards for the rights and freedoms of data subjects).

195. *Id.* art. 9 ("Processing of special categories of personal data") (prohibiting the processing of such data and listing exceptions to the prohibition).

196. *See id.* (listing biometric information and genetic information among the list of special categories of personal data).

over the GDPR in an independent agency, called a "supervisory authority."[197] These agencies have numerous responsibilities and powers relating to the implementation and interpretation of the GDPR, enforcement, investigations, and more.[198] The agencies are required to receive and process complaints filed by data subjects against controllers or processors and have authority to impose administrative fines in substantial amounts.[199] Depending on the circumstances, a supervisory authority may impose fines of up to €20,000,000 or 4% of a company's annual global revenues.[200]

The GDPR also includes a private right of action for data subjects who believe their GDPR rights have been violated. Data subjects have the right to an "effective judicial remedy" against a controller or processor that the data subject believes infringed their GDPR rights.[201] This right includes the ability to obtain compensation for damages from the controller or processor.[202] Data subjects also have the right to an effective judicial remedy against supervisory authorities that make a decision adverse to the data subject or fail to process the data subject's complaint.[203]

2. Potential Templates for a Maine Consumer Privacy Model: The CCPA

In 2018, California became the first state in the U.S. to enact a comprehensive consumer privacy law.[204] The state adopted the CCPA as an eleventh-hour compromise with Californians for Consumer Privacy, a nonprofit group that had developed a consumer privacy ballot initiative that Californians were expected to pass in the 2018 election cycle.[205] The group agreed to pull the initiative in exchange for the legislature enacting the CCPA.[206]

The CCPA regulates "businesses," a term defined to encompass companies that: (a) do business in California; and (b) have annual revenues exceeding $25 million, collect personal information from more than 50,000 California residents; or (c) derive 50% or more of their revenues from selling California residents' personal

---

197. *Id.* art. 51 ("Supervisory authority").

198. *Id.* arts. 57-58 ("Tasks" and "Powers," respectively).

199. *Id.* arts. 77, 83 ("Right to lodge a complaint with a supervisory authority" and "General conditions for imposing administrative fines," respectively).

200. *Id.* art. 83(5).

201. *Id.* art. 79 ("Right to an effective judicial remedy against a controller or processor").

202. *Id.* art. 82 ("Right to compensation and liability").

203. *Id.* art. 78 ("Right to an effective judicial remedy against a supervisory authority").

204. As I discuss later in this Section, in the 2020 election cycle California voters approved a ballot initiative called the California Privacy Rights Act ("CPRA"). That law significantly expands upon the CCPA's privacy protections such that California's privacy regime will look much like the GDPR when the core components of the CPRA go into effect in 2023. However, in this Section, I focus on the CCPA as originally enacted to provide Maine legislators and reformers with a contrast between two types of privacy regimes: the GDPR and the (original) CCPA.

205. *See* Stuart L. Pardau, *The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States?*, 23 J. TECH. L. & POL'Y 68, 89-91 (2018) (describing the circumstances surrounding Californians for Consumer Privacy's ballot initiative and the legislature's adoption of the CCPA); The California Consumer Privacy Act of 2018, 2017 Cal. A.B. 375 (West 2017), (codified as amended at CAL. CIV. CODE § 1798.100-198 (West 2018)); *Yes on 24,* CALIFORNIANS FOR CONSUMER PRIV., http://www.caprivacy.org [https://perma.cc/YE85-4HTJ] (last visited Apr. 11, 2021).

206. Pardau, *supra* note 205, at 90-91.

information.[207] The Act gives California residents—called "consumers"—certain rights to their "personal information," which is defined broadly to encompass any information reasonably capable of being associated with a consumer.[208]

The CCPA is sometimes called "California's GDPR," but the laws contain many important differences.[209] The rights created by the CCPA are more limited than those created by the GDPR, and the obligations imposed on covered businesses are concomitantly more limited as well. The CCPA also did not create a dedicated consumer privacy agency to implement and enforce the law. And, the private right of action provided by the CCPA is far more limited than the GDPR's.

Consumers have three main rights under the CCPA: the right to know, the right to delete, and the right to opt-out. The right to know is a transparency measure. It gives consumers the right to obtain from a business information about the personal information it has collected about the consumer.[210] This information includes the types of sources from which the business collects personal information, the purposes for which the company collects and sells personal information, the types of persons with whom the business shares personal information, and the categories and specific pieces of personal information collected.[211] The right to delete allows consumers to instruct businesses to delete their personal information, but the right contains many exceptions that allow businesses to decline a request to delete.[212] Lastly, the right to opt-out allows consumers to opt-out from the sale of their personal information.[213]

---

207. CAL. CIV. CODE § 1798.140(c)(1) (West 2018) (defining "Business"). "Businesses" under the CCPA are comparable to "controllers" under the GDPR. *See* GDPR, *supra* note 171, art 4. The CCPA also regulates service providers, which are comparable to "processors" under the GDPR. *See* § 1798.140(v) (defining "Service provider"); *see also* GDPR, *supra* note 171, art. 4.

208. See § 1798.140(g) (defining "consumer"); *id.* § 1798.140(o) (defining "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household," and listing several categories of information that may be personal information under the Act).

209. *See*, *GDPR & CCPA: Opt-ins, Consumer Control, and the Impact of Competition and Innovation: Hearing Before the U.S. S. Comm. on the Judiciary*, 116th Cong. 12 (2019) [hereinafter Richardson Testimony] (testimony of Michelle Richardson of the Center for Democracy & Technology) ("While the CCPA is often referred to as a 'Californian GDPR,' this is inaccurate."); Luke Irwin, *California's 'GDPR-Like' Privacy Law Passes: What You Need to Know*, IT GOVERNANCE USA BLOG (July 16, 2018), https://www.itgovernanceusa.com/blog/californias-gdpr-like-privacy-law-passes-what-you-need-to-know/ [https://perma.cc/66CM-L6F8] (referring to the CCPA as being similar to the GDPR); Richi Jennings, *CCPA, California's GDPR, Confuses and Confounds*, TECHBEACON, https://techbeacon.com/security/ccpa-californias-gdpr-confuses-confounds [https://perma.cc/P8YG-YZZE] (last visited Apr. 11, 2021) (same); Andy Patrizio, *While No One Was Looking, California Passed its Own GDPR*, NETWORK WORLD (July 5, 2018), https://www.networkworld.com/article/3286611/while-no-one-was-looking-california-passed-its-own-gdpr.html [https://perma.cc/6BBW-ZRXY] (same).

210. *See* CAL. CIV. CODE § 1798.110 (West 2020) (giving consumers the right to request information about their personal information from a business and obligating businesses to disclose such information).

211. *See id.* § 1798.110(a) (listing the types of information a consumer may request from a business).

212. *See id.* § 1798.105 (creating the right to delete and stating that a business need not comply with a request to delete in several circumstances, such as when the personal information is necessary to complete a transaction, detect a security incident, exercise free speech, comply with a legal obligation, or when the personal information is used for certain internal purposes).

213. *See id.* § 1798.120 (establishing the right to opt-out).

The obligations imposed on businesses mirror these rights. Businesses must provide a notice, at or before the point of collecting personal information, that discloses what personal information the business collects, the purposes for which the business uses the information, a link allowing consumers to opt-out from the sale of their personal information, and a link to the business's privacy policy.[214] A business's privacy policy must in turn contain an explanation of how consumers can submit requests to exercise their CCPA rights.[215] Businesses must also establish processes to receive and process consumers' requests to exercise their rights, including maintaining a "Do Not Sell My Information" link on their websites that allows consumers to opt-out of the sale of their personal information.[216]

These rights and obligations are narrower than those imposed by the GDPR. The right to know, delete, and opt-out parallel the GDPR's rights of access, erasure, and objection to direct marketing, but the CCPA does not contain a right to rectification, rights regarding automated decision-making or profiling, or rights regarding sensitive personal information (except children's information[217]). The CCPA also does not require businesses to establish a legal basis, such as consent, for processing personal information; businesses only need to provide notice—not obtain consent—before collecting information. Given the lack of a consent requirement, there is no right to object to processing under the CCPA.[218] Finally, the CCPA does not contain parallels to the GDPR's data minimization requirement or its data storage limitations. These omissions have led privacy advocates to criticize the law for placing too heavy a burden on consumers in policing how businesses use their personal information.[219]

The CCPA and the GDPR differ significantly when it comes to enforcement, as well. Unlike the GDPR, the CCPA did not create an independent agency for implementing and enforcing the law. The law instead vested that authority in the California Attorney General,[220] who may impose civil penalties up to $2,500 per

---

214. *See id.* § 1798.100 (establishing the notice requirement); CAL. CODE REGS. tit. 11, § 999.305(b) (2020) (listing the notice's required content).

215. *See* CAL. CIV. CODE. § 1798.130(a)(5) (listing content that is required to be included in a business's privacy policy, including a "description of a consumer's rights pursuant to [the CCPA] and two or more designated methods for submitting requests").

216. *See id* § 1798.130(a)(1)-(2) (requiring businesses to establish processes for consumers to submit requests for information and requiring businesses to respond to such requests within specified time limits); *id.* § 1798.135 (requiring businesses to maintain a "Do Not Sell My Personal Information" link that brings consumers to a web page where they can opt-out from the sale of their personal information).

217. The CCPA prohibits businesses from knowingly selling the personal information of children under 16 years-old unless the business obtains consent from: (a) the child's parent if the child is less than 13; or (b) the child if the child is 13, 14, or 15 years-old. CAL. CIV. CODE § 1798.120(c) (West 2020).

218. As noted directly above, the CCPA's right to opt-out does parallel the GDPR's right to object, but only to the extent the GDPR right applies to direct marketing of personal data.

219. *See, e.g.*, Richardson Testimony, *supra* note 209, at 12-13 (criticizing the CCPA as being "largely focused on transparency" rather than on limiting data collection and use). Indeed, Richardson is critical of both regulatory regimes for the burdens they place on consumers. *Id.* at 13-15. Relying on a notice or consent requirement "burdens individuals with navigating every notice, data policy, and setting, trying to make informed choices that align with their personal privacy interests." *Id.* at 14.

220. *See* CAL. CIV. CODE § 1798.185(a) (West 2020) (requiring the Attorney General to adopt regulations).

unintentional violation and $7,500 per intentional violation.[221] And, the CCPA provides only a limited private right of action to consumers. Consumers may only bring suit under the CCPA when a business's lax security practices lead to a data breach that causes the consumer harm.[222] The law establishes a statutory damages range of $100 - $750 per consumer, per incident, or actual damages, whichever is greater.[223] The CCPA does not give consumers a private right of action when a business violates the right to know, right to delete, or right to opt-out.

Many of the material differences between the CCPA and the GDPR may be short lived. In November 2020, Californians approved Prop. 24, the California Privacy Rights Act ("CPRA"), which amended the CCPA to bring consumers' rights and businesses' obligations in line with the GDPR's treatment of data subjects and controllers.[224] The CPRA also created a dedicated state agency to protect consumer privacy, the California Privacy Protection Agency.[225] While the provisions of the CPRA creating the new agency went into effect immediately, the new consumer rights are not effective until January 1, 2023.[226]

3. Maine Consumer Privacy Legislation

Maine's legislature has already recognized the importance of the privacy interests protected by the GDPR and the CCPA and has granted some of the rights provided by those laws. However, Maine has done so only for limited classes of people and in limited circumstances. The "Student Information Privacy Act" ("SIPA"), discussed above, provides a prime example. By enacting the SIPA, the legislature acknowledged the privacy risks created when companies use personal data for marketing purposes and accordingly prevented covered businesses from using students' data for such purposes.[227] Like the GDPR, the SIPA contains protections against profiling; a recognition that amassing personal data to gain insights into a person's preferences and behaviors can create a significant violation of privacy.[228] The SIPA prohibits the sale of student data and limits when such data can be disclosed to third parties, protecting similar privacy interests as the GDPR's

---

221. *Id.* § 1798.155(b).

222. *Id.* § 1798.150(a)(1) (authorizing a civil action for certain security breaches).

223. *Id.* § 1798.150(A) (creating the damages limitation).

224. *See* Cal. Sec'y of State, *Proposition 24 Amends Consumer Privacy Laws*, https://electionresults.sos.ca.gov/returns/maps/ballot-measures/prop/24 [https://perma.cc/G7ZD-GBEF] (last visited Apr. 27, 2021) (showing that Proposition 24 passed by a 56.2% – 43.8% margin); *California Proposition 24, Consumer Personal Information Law and Agency Initiative (2020)*, BALLOTPEDIA, https://ballotpedia.org/California_Proposition_24,_Consumer_Personal_Information_Law_and_Agency_Initiative_(2020) [https://perma.cc/HWR3-J7WC] (last visited Apr. 11, 2021) (showing that Proposition 24 passed by a 56.2% to 43.8% margin); Cal. Sec'y of State, *Proposition 24*, §§ 5-11, https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf [https://perma.cc/HV68-NZT2] (last visited Apr. 11, 2021) (establishing consumer rights).

225. Cal. Sec'y of State, *Proposition 24*, § 24, https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf [https://perma.cc/HV68-NZT2] (last visited Apr. 11, 2021) (establishing the California Privacy Protection Agency).

226. *Id.* § 31 (establishing the effective dates for various provisions of the CPRA).

227. *See* 20-A M.R.S.A. §§ 951-53 (Westlaw through 2019 2d Reg. Sess.).

228. *Id.* § 953(1)(B).

right to object and the CCPA's right to opt-out.[229] Finally, the SIPA requires covered businesses to implement reasonable security controls and requires businesses to delete students' data upon request.[230] The GDPR and the CCPA both impose similar obligations.[231]

Maine's groundbreaking legislation protecting the privacy of ISP customers likewise guards many of the same privacy interests as the GDPR and the CCPA. In enacting the ISP legislation, the legislature took the position that threats to privacy come not only from the exploitation of personal information like names, dates of birth, credit cards, and social security numbers, but also from technical information like device identifiers, application usage history, and IP addresses that can be used to track an individual's online behavior.[232] The legislation's broad definition of "customer personal information" encompasses these identifiers just as do the CCPA's and the GDPR's respective definitions of "personal information" and "personal data."[233] The legislation also contains notice and consent requirements and imposes cybersecurity obligations, all of which are similar to obligations found in either the GDPR or the CCPA.[234]

These laws, in sum, constitute a legislative recognition that certain classes of Mainers—K-12 students and ISP customers—have a privacy interest in controlling how their personal information is collected, used, shared, and sold. It is time for the legislature to recognize that all Maine residents hold these privacy interests and that a wide variety of businesses put these interests at risk. Maine should enact a general consumer privacy law.

The details of a Maine consumer privacy law would necessarily be the product of much legislative debate, input from privacy advocates and industry, and compromise. Here, I limit my recommendations to structural features of the law that I deem particularly desirable or important for the state. Lawmakers and reformers should view these recommendations as a starting point for the conversation around enacting a Maine consumer privacy law. I leave choices such as what specific rights to give consumers, whether to require businesses to establish a lawful basis before collecting personal information, and whether the law should apply to all persons that collect personal information (like the GDPR) or to a subset of businesses based on revenue or data-collection thresholds (like the CCPA) up to the legislative process.

Rulemaking Authority: A Maine consumer privacy law should give a state agency the power to promulgate regulations interpreting the law. Maine's recent

---

229. *Id.* § 953(1)(C)-(D); *see also id.* § 953(3) (listing exceptions to SIPA's disclosure restrictions).

230. *Id.* § 953(2)(B).

231. *See* GDPR, *supra* note 171, art. 17 ("Right to Erasure ('Right to be Forgotten')"); *id.* art. 32 ("Security of Processing") (requiring processors and controllers to implement "appropriate technical and organisational measures to ensure a level of security appropriate to the risk" posed by a breach of the personal data processed by the person); CAL CIV. CODE § 1798.105 (West 2020) (establishing the right to delete); CAL CIV. CODE § 1798.150 (West 2020) (incentivizing strong security practices by creating a private right of action when a consumer's "nonencrypted and nonredacted personal information" is breached as a result of the business's "violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information").

232. 35-A M.R.S.A. § 9301(1)(C) (Westlaw through 2019 2d Reg. Sess.).

233. *See* CAL. CIV. CODE § 1798.140(o)(1) (West, Westlaw through Ch. 2 of 2021 Reg. Sess.) (defining "personal information"); GDPR, *supra* note 171, art. 4(1) (defining "personal data").

234. 35-A M.R.S.A. § 9301(3), (6) (Westlaw through 2019 2d Reg. Sess.).

history of privacy reform illustrates why vesting such authority in a state agency is necessary. The history shows a legislature grappling with a near-impossible task: keeping up with advances in technology that move faster than a deliberative body can reasonably be expected to move.[235] Giving a state agency authority to clarify ambiguities in the law, to provide guidance on implementing the law, and to promulgate regulations applying the law to new technologies would go a long way toward mitigating the challenges inherent to legislating privacy protections.[236]

The most desirable option for allocating regulatory authority over consumer privacy would be to create a new agency dedicated to the task, much like EU member-states and California now have. A dedicated consumer privacy agency would be more capable of developing expertise in the area, working with industry, and enforcing the law than would an agency with numerous competing responsibilities. If, however, establishing a new state agency is politically untenable, then the legislature could grant regulatory and enforcement authority to the Office of the Maine Attorney General, given its relevant experience with enforcement and rulemaking for Maine's consumer protection laws and the state's data breach law.[237]

Private Right of Action: The law should include a private right of action rather than rely solely on agency actions for enforcement. A private right of action would allow consumers to vindicate their own privacy rights rather than be dependent on an agency to act. Further, enforcement actions can be expensive and time-consuming, particularly when an action is brought against a large tech company that can afford an army of lawyers. In a state with limited resources, like Maine, a private right of action can save costs by shifting some of the enforcement burden to private sector attorneys and advocacy groups.

A private right of action would likely draw pushback from industry and industry allies in the legislature.[238] New privacy laws can be difficult for companies to

---

235. *Cf.* Anne T. McKenna, *Pass Parallel Privacy Standards or Privacy Perishes*, 65 RUTGERS L. REV. 1041, 1085 (2013) ("[O]ne consistent failing in privacy legislation has been that legislation is drafted in technology-specific terms or technology-specific application; given the pace of advancements in technology, this has resulted in outdated and inapplicable portions of law."); Michael T. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 374-75 (2019) (describing the "legal lag" that occurs "when laws fall behind disruptive societal developments, such as rapid technological change").

236. *Cf.* CTR. FOR DEMOCRACY & TECH., FEDERAL BASELINE PRIVACY LEGISLATION DISCUSSION DRAFT (Dec. 5, 2018), https://cdt.org/wp-content/uploads/2018/12/2018-12-12-CDT-Privacy-Discussion-Draft-Final.pdf [https://perma.cc/S3NH-CWA3] (proposing federal privacy legislation that gives the Federal Trade Commission rulemaking authority).

237. *See* 5 M.R.S.A. § 207 (2020) (giving the Attorney General authority to make rules and regulations interpreting the Maine Unfair Trade Practices Act's prohibition on unfair or deceptive acts or practices); 10 M.R.S.A. §§ 1349, 1350-A (2020) (dividing enforcement and rulemaking authority over Maine's data breach law between the Department of Professional and Financial Regulation and the Attorney General).

238. The inclusion of a private right of action has been a major sticking point in the State of Washington's proposed Privacy Act. "Privacy advocates argue that a private right of action is essential for consumers to adequately enforce their privacy rights. Conversely, business advocates argue that a private right of action (particularly, one that allows for attorney's fees) would result in endless litigation." Megan Herr, Malia Rogers, & David M. Stauss, *Washington Privacy Act Update: Private Right of Action Added in House*, SECURITY MAGAZINE (Mar. 4, 2020), https://www.securitymagazine.com/articles/91834-washington-privacy-act-update-private-right-of-action-added-in-house [https://perma.cc/3WW7-ZQZZ].

implement, and not every technical violation of a consumer privacy law should necessarily result in civil liability. The legislature can strike the appropriate balance between its compliance goals and these industry concerns by qualifying the private right of action. I suggest three limitations.

First, the law could include a one-year grace period to give companies time to implement and operationalize the law without fear of incurring civil liabilities.[239] Second, the law could impose a scienter requirement for actions based on a company's violation of the law's individual privacy rights. Such actions could be cognizable only when the company acted with gross negligence, recklessness, or intentional misconduct. This scienter requirement would prevent litigants from seeking damages for violations caused by ordinary mistakes made during the process of disclosing information, removing someone from a marketing list, deleting someone's information, and the like. In contrast, private actions for data breaches could carry a negligence standard—similar to the CCPA's standard—to incentivize best security practices and to protect consumers from the risks of identity theft and exposure of sensitive personal information.[240] Third, the law could specify a damages range similar to the CCPA's range of $100 - $750, or actual damages, whichever is greater.[241] Harms posed by privacy violations are difficult to quantify.[242] Creating a statutory range will reduce uncertainty and make it easier for individual plaintiffs to vindicate their privacy rights.[243]

Automated Decision-Making: Creating basic rules for products and services that incorporate automated decision-making technologies is particularly important for Maine at this time. In early 2020, Northeastern University announced the opening of the Roux Institute in Portland.[244] The Institute provides graduate-level programs in several disciplines that revolve around automated decision-making technologies.[245] Indeed, the impetus for Lewiston native David Roux's $100 million donation to open the Institute was to grow the state's technology sector by

---

239. The CCPA contained a similar provision, delaying enforcement of the Act for six months after its effective date. *See* CAL. CIV. CODE § 1798.185(c) (West 2018) ("The Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner.").

240. *See* CAL. CIV. CODE § 1798.150(a)(1) (West, Westlaw through Ch. 372 of 2020 Reg. Sess.) (authorizing a civil action for certain data breaches caused by a "business's violation of the duty to implement and maintain reasonable security procedures and practices").

241. *Id.* § 1798.150(a)(1)(A).

242. *See, e.g.*, Jacqueline D. Lipton, *Mapping Online Privacy*, 104 NW. U. L. REV. 477, 486 (2010) (noting that "American tort law in particular tends to focus on identifying and compensating harms that can be economically quantified," and that "[i]t is difficult to quantify many privacy harms in this way."); Andrew J. McClurg, *A Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 118 (2003) (commenting that "the value of the data profile of any particular individual is small and difficult to quantify," and that "requiring victims of consumer profiling to prove a specific monetary loss [thus] unwarrantedly prejudices their claims.").

243. *See* McClurg, *supra* note 242.

244. Willis Ryder Arnold, *Northeastern University Launches $100 Million High-Tech Graduate Institute in Portland*, ME. PUB. RADIO (Jan. 27, 2020), https://www.mainepublic.org/post/northeastern-university-launches-100-million-high-tech-graduate-institute-portland [https://perma.cc/73SD-D4Y2].

245. *See Take Your Academics in a Brave New Direction*, THE ROUX INSTIT. AT NE UNIV., https://roux.northeastern.edu/academics [https://perma.cc/YWW3-U8TU] (last visited Apr. 11, 2021) (listing Experiential AI, Computer and Data Sciences, Digital Engineering, and Bioinformatics among the Institute's field of studies).

"work[ing] with Maine-based companies and provid[ing] certificates, master's degrees, and Ph.D.s in artificial intelligence and machine learning."[246]

The Roux Institute promises to be a boon for the state's economy, but the industry it will foster would benefit from some safeguards to protect residents from externalities associated with automated decision-making technologies. Left unchecked, such technologies can inadvertently (or intentionally) be used to exacerbate existing social inequities and to create new ones.[247]

In her book, *Weapons of Math Destruction*, Cathy O'Neil identifies a harmful subset of automated decision-making technologies that she calls "WMDs." As she explains, WMDs "encode[] human prejudice, misunderstanding, and bias" and tend to "punish the poor and oppressed in our society, while making the rich richer."[248] These dangerous automated decision-making technologies tend to share three common characteristics.

First, WMDs are opaque. Subjects may be unaware that automated decision-making technology is being used to make a decision about them.[249] And, even if they are aware of the technology, they are usually unaware of what inputs the algorithm uses to make decisions about them and how those inputs are weighed.[250] The lack of transparency makes it difficult to assess whether a decision-making technology produces unfair results, limits a subject's ability to challenge the results, and can "lead to a feeling of unfairness" even if the technology is otherwise fair.[251]

Second, WMDs are damaging: they work against the subject's interest, produce unfair results, and damage or destroy lives.[252] This damage is usually caused by a "feedback loop" in the WMD, which occurs when a decision-making technology lacks feedback to inform whether the decisions it makes are correct.[253] Without feedback, WMDs cannot "learn[] from [their] mistakes" and instead create their own truths—a teacher is bad because the technology says he is bad, a criminal is dangerous because the technology says she is dangerous, a job applicant is unreliable because the technology says he is unreliable—and none of these decisions are evaluated for accuracy so the technology can be adjusted and improved.[254]

---

246. Arnold, *supra* note 244.

247. *See generally* CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016) (identifying a harmful subset of automated decision-making technologies that O'Neil calls "WMDs"); FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? 8-10 (Jan. 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf [https://perma.cc/VA3E-B78B] (listing the ways in which "potential inaccuracies and biases" with big data "might lead to detrimental effects for low-income and underserved populations"); RUHA BENJAMIN, RACE AFTER TECHNOLOGY (2019) (detailing how the use of big data in automated decision-making technologies perpetuates systemic racial biases and inequities).

248. O'NEIL, *supra* note 247, at 3.

249. *See id.* at 28-29 (describing WMDs as being opaque or invisible).

250. *See id.* at 28 ("We're modeled as shoppers and couch potatoes, as patients and loan applicants, and very little of this do we see . . . .").

251. *Id.* at 10, 28-29 ("But you cannot appeal to a WMD. That's part of their fearsome power. They do not listen. Nor do they bend. . . . [T]he programs deliver unflinching verdicts, and the human beings employing them can only shrug, as if to say 'Hey, what can you do?'").

252. *See id.* at 29.

253. *See id.* at 6-7.

254. *Id.*

Third, WMDs are scalable.[255] When a WMD has the capacity to "grow exponentially" a "local nuisance[]" can become a "tsunami force[]" that produces unfair results across whole sectors of the economy and society.[256]

Examples of WMDs, as O'Neil details, are legion. WMDs rank universities,[257] determine what advertisements we see (often to the detriment of the poor and oppressed),[258] identify which neighborhoods to (over)police,[259] and make a range of financially consequential decisions regarding employment, access to credit, and insurance.[260]

How do we curb the reach of existing WMDs and prevent the promising big-data industry in Maine from becoming a laboratory for new ones? Fortunately, there is a menu of options from which the legislature can choose. O'Neil's recommendations include requiring that automated decision-making technologies be regularly audited for accuracy and fairness; imposing transparency measures to allow consumers to better understand how the technologies make decisions; and expanding existing laws that regulate credit reporting agencies, heath care data, and discrimination to encompass more products that rely on automated decision-making technologies.[261]

The GDPR creates a default rule that decisions "based solely on automated processing" that produce "legal effects" or "similarly significant[]" effects are prohibited.[262] Companies can avoid this rule only when automated processing is necessary for the performance of a contract, authorized by law, or based on the subject's consent. Even in such situations, national law and the controller must provide "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests."[263] At a minimum, controllers must provide the data subject the right to obtain human intervention in the decision-making and to contest the decision.[264]

Finally, the newly-enacted CPRA requires the California Privacy Protection Agency to address automated decision-making technologies via regulation. The Agency must promulgate regulations "governing access and opt-out rights with respect to businesses' use of automated decision-making technology" including the right to receive "meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer."[265]

---

255. *Id.* at 29-30.

256. *Id.* at 30.

257. *See id.* at Ch. 3 (arguing that the U.S. News's model for ranking colleges and universities is a WMD).

258. *See id.* at Ch. 4 (explaining how for-profit colleges target misleading advertisements to poor Americans).

259. *See id.* at Ch. 5 (detailing how the use of crime-prediction programs creates a feedback loop whereby increased arrests in impoverished neighborhoods leads to over-policing in those neighborhoods).

260. *See id.* at Chs. 6-7 (employment), Ch. 8 (credit), Ch. 9 (insurance).

261. *Id.* at 208-14.

262. GDPR, *supra* note 171, art. 22.

263. *Id.*

264. *Id.*

265. *California Privacy Rights Act*, California Proposition 24 § 21 (2020).

I recommend taking elements from each of these (somewhat overlapping) approaches to regulating automated decision-making technologies. Specifically, Maine should require companies to regularly audit technologies that make automated decisions about important aspects of life; empower consumers to obtain human intervention and to contest automated decisions; and endow a regulatory agency with rulemaking authority to adjust the rules for this rapidly evolving technology. Additional protections for automated decisions based on sensitive personal characteristics like race, religion, and gender, and based on proxies for such characteristics, would also be desirable.

Targeted Advertising: The digital advertising industry is a complex information ecosystem. Content publishers—such as websites, social media platforms, search engines, and video platforms—collect vast amounts of personal information from users and then use that information to allow advertisers to target their ads to highly specific segments of the platform's user-base.[266] Users' personal information is also made available to specialized service providers that assist content publishers and advertisers in facilitating ad placements or optimizing ad campaigns.[267] The collection, use, and exchange of personal information adds up to a highly lucrative and highly effective digital advertising industry.[268] The ability to target digital ads based on user personal information is the backbone of the industry.[269]

A lack of clarity in the CCPA regarding whether targeted advertising involves the "sale" of personal information, as that term is defined by the CCPA, has caused needless uncertainty and confusion in the implementation of that law.[270] For example, two of the world's largest tech companies, Google and Facebook, have taken opposite positions on whether targeted advertising involves a sale of personal information under the CCPA and whether consumers thus have a right to opt-out from targeted advertising.[271] The Interactive Advertising Bureau ("IAB"), a digital advertising industry group, has created a complex CCPA framework in an attempt to avoid violating the law if California's Attorney General does interpret the term "sale" to apply to targeted advertising.[272] But this attempt to avoid "selling" personal

---

266. Kyle Langvardt, *Regulating Habit-Forming Technology*, 88 FORDHAM L. REV. 129, 137 (2019) ("[T]argeting requires advertisers to collect as much data as possible about the user—not only demographic data, but minute-by-minute data about the user's location, mood, and desires.").

267. *See generally* Dina Srinivasan, *Why Google Dominates Advertising Markets Competition Policy Should Lean on the Principles of Financial Market Regulation*, 24 STAN. TECH. L. REV. 55, 70-76 (2020) (describing the marketplace in which advertisers and publishers purchase and sell digital ads).

268. Russell A. Miller, *The Legal Fate of Internet Ad-Blocking*, 24 B.U. J. SCI. & TECH. L. 299, 306-07 (2018) (describing the "mind-boggling growth" of internet advertising revenue).

269. *See id.* at 307 (describing how online advertising is particularly valuable to marketers because "digital ads can strategically target consumers in ways that ads in traditional media cannot.").

270. CAL. CIV. CODE § 1798.140(t)(1) (West 2020) (defining "sale" as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration.").

271. Patience Haggin, *Facebook Won't Change Web Tracking in Response to California Privacy Law*, WALL ST. J. (Dec. 12, 2019, 1:29 PM), https://www.wsj.com/articles/facebook-wont-change-web-tracking-in-response-to-california-privacy-law-11576175345 [https://perma.cc/LR6Q-PP3Z] (contrasting Facebook's position regarding the CCPA's definition of "sale" with Google's position).

272. Interactive Advert. Bureau, *IAB CCPA Compliance Framework for Publishers & Technology Companies Version 1.0*, (Dec. 4, 2019), https://www.iab.com/wp-content/uploads/2019/12/IAB_CCPA-

information without disrupting the above-described information ecosystem has drawn criticism from Californians for Consumer Privacy, which believes the IAB's framework still runs afoul of consumers' right to opt-out from sales.[273]

Maine should avoid this confusion by clearly stating how the prospective consumer privacy law applies to business's use of personal information in targeted advertising. One option would be to create a specific right to opt-out from targeted advertising and to clearly explain what happens when a consumer exercises that right. In particular, the law should explain what personal information can and cannot be used for advertising purposes once a user opts-out. The opt-out right could be structured such that platforms cannot use any personal information for targeting ads once a user opts-out. Or, the opt-out could be narrowed such that platforms could still target ads based on a limited set of personal information that poses minimal privacy risks.[274] Regardless of the ultimate contours of the opt-out right, the legislature should make those contours clear to avoid the type of uncertainty caused by the CCPA.

Updating Maine's Breach Notification Statute: As part of a general consumer privacy law, Maine should update its data breach notification statute to provide consumers with greater protections in the event of a breach. First, Maine should expand the statute's definition of "personal information." Currently, the term only covers basic types of personal information that lead to a risk of identity theft when breached: social security numbers, driver's license numbers, account numbers and passwords, and the like.[275] Companies that experience breaches of other types of personal information thus do not need to report the breach to consumers under Maine law.

The scope of the statute's definition of personal information made sense when it was enacted in 2005, as the legislature's chief concern was preventing identity theft caused by data breaches. However, companies today are collecting many more types of personal information and breaches of such information can have consequences beyond identity theft. Other states thus maintain breach notification laws with definitions of personal information that encompass categories such as biometric information, DNA profiles, medical or health information, certain electronic

---

Compliance-Framework-for-Publishers-Technology-Companies.pdf [https://perma.cc/YJZ2-PXEV]. Under the Framework, when a consumer opts-out from the sale of their personal information, the content publisher automatically sends a signal to all of the downstream companies involved in targeting advertisements on the publisher's platform. The signal triggers a series of contractual arrangements that restrict how the downstream companies can use the consumer's personal information. *Id.* As of this writing, it is unclear whether the contractual arrangements created by the Framework comply with the CCPA's opt-out requirements.

273. *See Californians for Consumer Privacy Comments on IAB's Proposed CCPA Framework*, CALIFORNIANS FOR CONSUMER PRIV. (Nov. 5, 2019), https://www.caprivacy.org/californians-for-consumer-privacy-comments-on-iabs-proposed-ccpa-framework/ [https://perma.cc/K8ZQ-GBXD] (arguing that the Framework "would contravene certain express tenets of CCPA").

274. For example, advertisements could continue to be targeted based on how users engage with the platform during their web-session (e.g., displaying an ad because someone clicked a particular link on a webpage); based on the website from which the user was referred to the platform (e.g., showing users a basketball-related advertisement when they visit a platform from NBA.com); and based on high-level geolocation information (e.g., showing a local advertisement to users located in Portland, Maine).

275. 10 M.R.S.A. § 1347(6) (2019).

identifiers, digital signatures, and work evaluations.[276] At a minimum, Maine should expand its definition of personal information to require companies to report breaches of biometric information, DNA profiles, and health information. Consumers ought to know when an unauthorized party accesses these categories of deeply personal information.

Second, Maine's breach notification law does not provide a private right of action, relying instead on the DPFR or the Attorney General to protect consumers through enforcement actions. Maine could empower consumers to vindicate their own rights by adopting the DPFR's 2006 recommendation and providing a limited private right of action for actual damages caused by the failure to investigate or timely notify consumers of a breach.[277] Many other states and territories already provide their residents with a private right of action for violations of data breach notification laws in certain circumstances.[278]

***

Fortunately, Maine already has a Maine-specific legislative model from which to draw in fashioning a consumer privacy law for the state. During the committee proceedings for Maine's ISP legislation, an amendment that would have replaced the bill with a general consumer privacy law was introduced and defeated.[279] The amendment would have (1) imposed disclosure obligations on businesses that collect personal information,[280] (2) given consumers rights to know and to opt-out similar to Californians' parallel CCPA rights,[281] (3) required businesses to conduct risk assessments regarding their use of personal information,[282] and (4) allowed the Attorney General to enforce the law through civil actions.[283] To be sure, this failed amendment would need revising to conform to the suggestions I offer here, but it presents a good foundation from which to build a law that adequately safeguards the privacy of Maine residents.

---

276. *See, e.g.*, ARIZ. REV. STAT. § 18-551(11)(f), (l) (2020) (including medical information and biometric information in the definition of "specific data element"); DEL. CODE ANN. tit. 6, § 12B-101(7)(a)(6), (8) (2018) (including medical information and biometric information); FLA. STAT. § 501.171(1)(g)(1)(a)(IV) (2020) (including medical information); 815 ILL. COMP. STAT. ANN. 530/5(1)(D) (LexisNexis 2020) (including medical information); N.C. GEN. STAT. § 75-61(10) (2020); N.D. CENT. CODE § 51-30-01(4)(a)(7), (10) (2019) (including medical information and digital signatures); P.R. LAWS ANN. tit. 10, § 4051(a)(5), (7) (2020) (including medical information and work-related evaluations); WIS. STAT. § 134.98(1)(b)(4)-(5) (2020) (including DNA profile and biometric data).

277. *See supra* notes 109-111 and accompanying text (discussing the DPFR's report).

278. *See, e.g.*, *Breach Notification Law Interactive Map*, BAKER & HOSTETLER LLP, https://www.bakerlaw.com/BreachNotificationLawMap [https://perma.cc/RL77-P9XY] (last visited Apr. 11, 2021) (showing over a dozen states and territories that provide a private right of action).

279. *See An Act to Protect the Privacy of Online Customer Information: Hearing on L.D. 946 Before the Comm. on Energy, Utilities and Tech.,* 129th Legis. 112-118 (Me. 2019), *available from* Me. State Law & Leg. Reference Library by requesting cf129-LD-0946.pdf.

280. *Id.* § 172(1).

281. *Id.* § 172(2)-(3).

282. *Id.* § 173.

283. *Id.* § 176.

B. Mitigating Specific Privacy Threats

To supplement a general consumer privacy law, Maine should continue to address privacy threats posed by emerging technologies, as the state has done repeatedly in the past. Responses to new technologies can come in the form of amendments to the general consumer privacy law, additions or amendments to other sections of Maine law, or through regulations promulgated by the state agency vested with rulemaking authority under the general consumer privacy law. In this Section, I identify five privacy threats caused or exacerbated by recent advances in technology that warrant a specific legislative or regulatory response from the state: (1) facial recognition technology; (2) biometric information; (3) smart-home devices; (4) data brokers; and (5) the Maine Information and Analysis Center.

Facial Recognition Technology: Facial recognition technology, or facial surveillance technology, "uses algorithms designed to analyze images of human faces" to allow the user to identify a person based on an image of their face.[284] "In one form of facial surveillance technology," for example, "a computer program analyzes an image of a person's face, taking measurements of their facial features to create a unique 'faceprint.'"[285] These faceprints can then be used "in combination with databases like the driver's license system at the Bureau of Motor Vehicles and surveillance camera networks, to identify and track people en masse."[286]

The technology poses serious risks to privacy and liberty when it is used by law enforcement and other government agencies. Facial recognition can be paired with networks of public surveillance cameras to "easily and continuously track everyone's public movements," threatening the conditions that allow fundamental freedoms like speech, association, and religion.[287] The technology can also exacerbate existing social inequities and create new ones. For example, face surveillance systems used by law enforcement often compare images against mugshot databases. Because Black and Latino people are historically more likely to be arrested than white people for committing the same crimes, "[u]sing mugshot databases for face surveillance searches exacerbates historical inequities by recycling that bias through new technology, and unfairly scrutinizing people who have long been targets of disproportionate police attention."[288] Recognizing these dangers, cities such as San Francisco, Oakland, and Boston have banned city agencies from using facial recognition technology, while other cities and states have implemented partial restrictions.[289]

In Maine, the City of Portland has been a leader on this front. The City Council

---

284. Michael Kebede, *An Open Letter to Portland City Council on Facial Recognition*, ACLU OF ME. (Jan. 6, 2020), https://www.aclumaine.org/en/news/open-letter-portland-city-council-facial-recognition [https://perma.cc/9UGS-UYGY].

285. *Id.*

286. *Id.*

287. *Id.* (arguing that the use of face surveillance technologies poses a threat to First, Fourth, and Fourteenth Amendment rights).

288. *Id.*

289. *See id.* (listing state localities that have banned law enforcement use of facial recognition technology); Ally Jarmanning, *Boston Bans Use of Facial Recognition Technology. It's the 2nd-Largest City To Do So*, WBUR (June 24, 2020), https://www.wbur.org/news/2020/06/23/boston-facial-recognition-ban [https://perma.cc/Y6ZU-92B5].

unanimously voted to ban the use of facial recognition technology by the city and by city officials in August 2020.[290] Two months later, voters approved a ballot initiative that replaced the city's prohibition on facial recognition technology in favor of a prohibition with more stringent enforcement mechanisms.[291] The initiative, Question B, includes a private right of action against the City of Portland and includes a bar on using evidence obtained in violation of the section in court.[292]

Maine should regulate government use of facial surveillance technology on the state level to create a uniform policy. There is no reason why a person in Portland should have greater protections for their privacy than someone a couple miles down the road in Westbrook or a couple hundred miles up the road in Caribou. Indeed, the legislature has already indicated that the privacy intrusions posed by facial surveillance technology require a state-level solution. The state's "Act to Protect the Privacy of Citizens from Domestic Unmanned Aerial Vehicle" prohibits the use of facial recognition technology in drones.[293] The legislature should extend that prohibition to all other mediums and prohibit the government from using facial recognition entirely.[294]

Proponents of the technology may assert that the government should be allowed to install facial surveillance systems and to access the systems in emergency situations. But, "emergency powers . . . tend to kindle emergencies."[295] In my view, the risk is too high that, if facial recognition technology is allowed to be deployed, established safeguards will be eroded and the creep of authoritarianism will persist.

Biometric Information: There is perhaps no type of information more *personal* than information about your person.[296] New technologies can collect and use identifying information about your face, eyes, voice, and fingerprints; data about your sleep habits, breathing pattern, and heart rate; and even your unique human genome.[297] These technologies have their benefits but carry attendant privacy risks.

---

290. Portland, Me., Code §§ 17-129 to -132 (Aug. 3, 2020).

291. Question B, An Act to Ban Facial Surveillance by Public Officials in Portland, PORTLAND, ME., https://www.portlandmaine.gov/DocumentCenter/View/29039/Ballot-Question-Initiative-language-Nov-2020 [https://perma.cc/R89Q-NUUD] (last visited Apr. 11, 2021).

292. *Id.* § 17-132.

293. Me. P.L. 2015, ch. 307, § 1 (codified at 25 M.R.S.A. § 4501(5)(D)).

294. Like the City of Boston's ban on facial surveillance technologies, narrow carve-outs can be established for using the technology for user authentication. *See* Boston, Ma., Ordinance Docket 0683 (June 24, 2020), Ordinance Banning Face Surveillance Technology in Boston, http://meetingrecords.cityofboston.gov/sirepub/mtgviewer.aspx?meetid=511&doctype=minutes&itemid=33202 [https://perma.cc/QRR2-N39Z] (last visited Apr. 11, 2021) (codified at BOSTON, MA., MUN. CODE §16-62 (2020)).

295. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 650 (1952) (Jackson, J., concurring).

296. Indeed, the Supreme Court has long interpreted the Constitution to include privacy protections for decisions about the body. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 485 (1965) (holding that the Constitution includes a right to privacy that protects a married couple's ability to be counseled in the use of contraceptives); Roe v. Wade, 410 U.S. 113, 153 (1973) (holding that the Constitution's right of privacy "is broad enough to encompass a woman's decision whether or not to terminate her pregnancy").

297. *See, e.g.*, ZUBOFF, *supra* note 122, at 236 (describing a "smart" mattress that collects data on users' heart rates, breathing, and movements); *id.* at 246 (describing biometric data that can be collected through wearable technologies); IGO, *supra* note 2, at 359 (describing how biometric identifiers such as facial recognition, fingerprinting, retina scanning, voice spectrometry, and DNA typing have "migrated from criminal justice into the society at large in recent decades"); Scott R. Peppet, *Regulating the*

Just like other types of personal information, biometric information collected by companies can be used and shared for purposes beyond what consumers would reasonably expect. Because the information is deeply personal and immutable, the harms posed by such misuses of biometric information can be substantial.

These concerns have led Illinois, Washington, and Texas to specifically regulate the use of some biometric information.[298] The most important of these laws is the Illinois "Biometric Information Privacy Act" ("BIPA"). Unlike the biometric information privacy laws enacted by Washington and Texas, Illinois included a private right of action, which has led to suits against companies including Facebook, Google, and Shutterfly.[299]

The BIPA defines biometric information to encompass information about retina or iris scans, fingerprints, voiceprints, and scans of the "hand or face geometry."[300] The law imposes five restrictions on companies that collect such information. First, companies must receive consent prior to collecting or otherwise obtaining biometric information.[301] Second, companies are prohibited from selling or otherwise profiting from a person's biometric information.[302] Third, companies must obtain consent before disclosing biometric information to another party.[303] Fourth, the law imposes a "reasonable standard of care" on companies to safeguard biometric information.[304] Finally, companies must maintain a written policy providing that biometric information be destroyed upon the earlier of: (a) the date on which the original purpose for collecting the information has been satisfied; and (b) three years from the individual's last interaction with the company.[305]

Maine should enact a biometric information privacy law similar to the BIPA but with a broader definition of "biometric information." When Illinois enacted the BIPA it was chiefly concerned with the use of biometric information for identity verification in financial transactions and security screenings.[306] These identity

---

Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 TEX. L. REV. 85, 88 (2014) (listing numerous devices that collect biometric information).

298. For example, when Illinois enacted the state's Biometric Information Privacy Act ("BIPA"), the legislature expressed a particular concern for the privacy risks posed by requiring consumers to verify their identities via biometric information in order to access a financial account. *See* 740 ILL. COMP. STAT. §§ 14/1-99 (2008). "Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *Id.* § 14/5. The legislature also declared that regulating biometric information as necessary because "[t]he full ramifications of biometric technology are not fully known." *Id.*

299. *In re* Facebook Biometric Info. Priv. Litig., 185 F. Supp. 3d 1155 (N.D. Cal. 2016); Rivera v. Google, Inc., 238 F. Supp. 3d 1088 (N.D. Ill. 2017); Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 WL 4099846 (N.D. Ill. Sept. 15, 2017).

300. 740 ILL. COMP. STAT. ANN. § 14/10.

301. *See id.* § 14/15(b).

302. *See id.* § 14/15(c).

303. *See id.* § 14/15(d). This consent requirement contains narrow exceptions for certain financial transactions, disclosures required by law, and disclosures required by a warrant or subpoena. *Id.*

304. *Id.* § 14/15(e).

305. *See id.* § 14/15(a).

306. *See id.* § 14/5(a) ("The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.").

verification services generally rely on the types of biometric information listed in the BIPA. However, companies are now using a broader range of biometric information for a wider variety of purposes; a trend that is almost certain to continue. Maine's biometric information law should reflect this development.

Smart-Home Devices: The home has been considered the penultimate zone of privacy for centuries.[307] In the common law and in American constitutional law, courts have employed the maxim that a "person's house is their castle" to guard the home from unwanted government intrusions.[308] The home is also expected to be secured from the intrusions of private parties. Through the physical construction of homes with solid doors and window curtains to social customs like knocking before entering, our culture has made a home's occupant the master of who may view and access their home's interior.[309] This authority is enshrined by trespass, nuisance, burglary, criminal invasion of privacy, and similar laws providing relief for unwanted intrusions on real property.

In recent years, the sanctuary of the home has come under threat from a growing body of devices that collect information from the home's interior. These smart-home devices include internet-connected security systems, lights, refrigerators, heating and cooling systems, vacuums, televisions, door-locks, and more.[310] Smart-home devices collect data from the home and transmit that data to the device manufacturer who can monetize it in several ways.[311] For example, in 2017 iRobot announced that

---

307. *See, e.g.*, William Pitt, Earl of Chatham, Speech on the Excise Bill, House of Commons (Mar. 1763) ("The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storm may enter; the rain may enter; but the King of England cannot enter—all his force dares not cross the threshold of the ruined tenement!"), *quoted in* Miller v. United States, 357 U.S. 301, 307 (1958).

308. *See, e.g.*, *Miller*, 357 U.S. at 306-07 ("From earliest days, the common law drastically limited the authority of law officers to break the door of a house to effect an arrest. Such action invades the precious interest of privacy summed up in the ancient adage that a man's house is his castle."); Payton v. New York, 445 U.S. 573, 596-97 (1980) ("The zealous and frequent repetition of the adage that a 'man's house is his castle,' made it abundantly clear that both in England and in the Colonies 'the freedom of one's house' was one of the most vital elements of English liberty."); Georgia v. Randolph, 547 U.S. 103, 115 (2006) ("We have . . . lived our whole national history with an understanding of 'the ancient adage that a man's house is his castle . . . .'"). I have intentionally removed the gendered language from the adage in the body of this article to avoid perpetuating its inherent sexism. I have left the original language in the cases cited in this footnote for historical accuracy.

309. Customs regarding household privacy vary by culture. In *Privacy and Freedom*, Westin describes a contemporaneous study of Javanese households to provide a contrast to household privacy norms in the U.S. In Java, "[t]he houses face the street with a cleared front yard in front of them. There are no walls or fences around them, the house walls are thinly and loosely woven, and there are commonly not even doors. Within the house people wander freely just about any place any time, and even outsiders wander in fairly freely almost any time during the day and early evening." WESTIN, *supra* note 2, at 16 (quoting a study by Clifford Geertz comparing household-privacy practices in Bali and Java). However, even in societies where persons freely enter each other's homes, "there will usually be rules limiting what a person may touch or where he may go within the house. There will also be norms limiting family conversation or acts performed while the outsiders are present." *Id.* at 15.

310. Smart-home devices constitute a subset of devices that are commonly referred to as the "Internet of Things" (IoT). *See, e.g.*, Peppet, *supra* note 297, at 88-89 (listing IoT devices including household devices such as thermostats, ovens, refrigerators, and home electricity and water-usage trackers).

311. *See, e.g.*, Fed. Trade Comm'n, Comments of the Electronic Privacy Information Center to the FTC on the Privacy and Security Implications of the Internet of Things, 12 (June 1, 2013),

it would monetize floor plans of consumers' homes created from the Roomba's mapping technology.[312] The company then equipped the vacuum with new sensors, cameras, and software to facilitate its mapping function.[313] Vizio used its line of smart TVs to capture billions of data points about users' viewing habits then sold users' viewing histories to advertisers and others.[314] By 2015, Samsung's smart TVs were "recording everything said in the vicinity of the TV" and sending the recordings to be transcribed by a third party.[315] A participant in the FTC's 2015 study on the "Internet of Things" ("IoT") shared that fewer than 10,000 households using their company's interior-home device generated 150 million data points, or "approximately one data point every six seconds for each household."[316]

The astounding amount of personal data collected from the home's interior by smart-home appliances is surpassed only by another type of smart-home device: the digital personal assistant. A digital personal assistant serves two primary functions for the user. First, it is the central nervous system for the home's other smart-home devices. The personal assistant integrates with the home's smart lights, cameras, locks, and appliances such that a user can control all these things with a voice command—*"Hey Google, turn on the lights." "Hey Alexa, change the channel."* Second, the personal assistant allows the user to conduct a variety of daily tasks through voice commands, including searching the internet, playing music, ordering goods, calling friends, and more.

These functions combine to allow the companies that produce digital personal assistants to monetize data about "a theoretically limitless scope of animate and inanimate domestic activities: conversations, lightbulbs, queries, schedules, movement, travel planning, heating systems, purchases, home security, health concerns, music, communication functions, and more."[317] Conversations and activities once thought to occur in the sanctuary of the home are thus "eagerly rendered as surplus" to be sold by the titans of industry to advertisers and other purchasers who may find such data useful.[318]

To be sure, homeowners willingly put these devices in their homes and often

---

https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf [https://perma.cc/NKS4-B8NN] [hereinafter "EPIC Comments"] ("Smart devices could reveal a wealth of information about consumers' location, media consumption, activity patterns, associations, lifestyle, age, income, gender, race, and health—information with potential commercial value. Companies might attempt to exploit this data by using it to target advertising or selling it directly.").

312. ZUBOFF, *supra* note 122, at 235; *see also* Josh Hafner & Edward C. Baig, *Your Roomba Already Maps Your Home. Now the CEO Plans to Sell the Map*, USA TODAY (July 25, 2017, 12:36 PM), https://www.usatoday.com/story/tech/nation-now/2017/07/25/roomba-plans-sell-maps-users-homes/508578001/ [https://perma.cc/8YW7-F35U] (quoting iRobot CEO Colin Angle as declaring that "there's an entire ecosystem of things and services that the smart home can deliver once you have a rich map of the home that the user has allowed to be shared").

313. ZUBOFF, *supra* note 122, at 235; Hafner & Baid, *supra* note 312.

314. ZUBOFF, *supra* note 122, at 265.

315. *Id.* at 264.

316. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 14 (FTC Staff Report 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/27QR-JJQJ] (last visited Apr. 11, 2021).

317. ZUBOFF, *supra* note 122, at 262.

318. *Id.* at 261.

find the devices beneficial or convenient. But this is no defense to the privacy intrusions posed by smart-home devices. Homeowners may not appreciate the extent to which the devices collect information or the extent to which companies use and share the information. In this sense, the devices exceed the scope of the owner's invitation into their home like a houseguest who snoops through their drawers or surreptitiously records their dinner conversation. They may also create an avenue for hackers to access the home's interior; a house-sitter who fails to safeguard your keys, if you will.[319]

Careful regulation is necessary to protect privacy in the home while also allowing homeowners to enjoy the benefits of smart-home devices. While there are different ways to strike this balance, I suggest incorporating three elements into legislation or regulation governing smart-home devices.

First, companies should be required to obtain consumers' express opt-in consent before using data from smart-home devices for secondary purposes such as targeted advertising or sales to third parties. Such uses are simply not in line with consumers' reasonable expectations and consumers should not be required to submit to having their interior-home data sold as a condition for using a smart-home device. This consent requirement could be paired with an anti-discrimination protection such that if the consumer declines to consent to the secondary use, the device must still function to the extent possible.[320]

Second, Maine should establish a data-minimization requirement for smart-home devices. Companies should only be allowed to collect information that is necessary or desirable for device functionality and improvement.[321] Your refrigerator probably does not need to record your conversations, track your music preferences, or log your travel schedule.

Third, if the state does not enact a general consumer privacy law that requires companies to take reasonable security measures and grants a private right of action for data breaches caused by a violation of that duty, the state should impose such a requirement on companies that produce smart-home devices given the security risks posed by a third-party gaining access to a consumer's locks, security cameras, thermostat, and more.[322]

Data Brokers: Data brokers are businesses that amass consumer personal information from sources other than consumers themselves and then sell that

---

319. *See* Hayley Peterson, *Wisconsin Couple Describe the Chilling Moment That a Hacker Cranked Up Their Heat and Started Talking to Them Through a Google Nest Camera in Their Kitchen*, BUS. INSIDER (Sept. 25, 2019, 4:12 PM), https://www.businessinsider.com/hacker-breaks-into-smart-home-google-nest-devices-terrorizes-couple-2019-9 [https://perma.cc/M7NY-D8VX]; Stephen Gandel, *Hackers Target Home Security Cameras: "I'm Coming for Your Baby"*, CBS NEWS (Dec. 13, 2019, 3:37 PM), https://www.cbsnews.com/news/ring-and-nest-hackers-home-security-cameras-vulnerable-to-cyberattacks/ [https://perma.cc/6GQU-ZMQM].

320. *See* EPIC Comments, *supra* note 311, at 18 (proposing a consent requirement and arguing that for consent to be effective "companies must not be allowed to condition use of a service on unnecessary data collection").

321. *See id.* at 20 (proposing a data minimization requirement).

322. California recently enacted legislation requiring all IoT devices to have reasonable security features. The legislation does not include a private right of action. CAL. CIV. CODE §§ 1798.91.04–.06 (West 2020).

personal information to third parties.[323] These companies collect data from public records, other publicly available sources, and commercial databases.[324] They then supplement this data with "certain derived data, which they infer about consumers."[325] For instance, "a data broker might infer that an individual with a boating license has an interest in boating."[326] By combining this collected and inferred information, data brokers can build detailed profiles of nearly every American adult, which can then be packaged into marketable products.

A 2014 Federal Trade Commission report examined nine data brokers who offer marketing products, risk mitigation products, or "people search" products. The marketing products allow companies to purchase information about their customers (or potential customers) to facilitate marketing efforts and to analyze their customer-base's data to improve ad targeting.[327] Risk mitigation products assist companies in confirming their customers' identities or in assessing the likelihood a particular transaction is fraudulent.[328] For example,

> data brokers offer their clients a quiz product, which typically includes questions to which the answers should be easily known to the consumer, but would not likely appear in information stolen by an identity thief . . . . Questions might include: "Which of these is an email address you have used?" or "What is your mother's birthday?"[329]

Lastly, "people-search" products allow users to search the data brokers' information database to locate information about a particular person.[330] Database information may include court records, property records, social media information, demographic information, and employment history.[331]

The amount of information data brokers collect and infer to create these products is truly astounding. "[O]ne data broker's database has information on 1.4 billion consumer transactions and over 700 billion aggregated data elements . . . another data broker adds three billion new records each month to its databases, . . . [while another] has 3000 data segments for nearly every U.S. consumer."[332]

The FTC's report confirmed the obvious: data brokers pose significant privacy

---

323. *See, e.g.*, CAL. CIV. CODE § 1798.99.80(d) (West 2020) (defining "data broker" as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship"); FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 3 (2014) [hereinafter "FTC DATA BROKERS REPORT"] (defining "data brokers" as "companies whose primary business is collecting personal information about consumers from a variety of sources and aggregating, analyzing, and sharing that information, or information derived from it, for purposes such as marketing products, verifying an individual's identity, or detecting fraud").

324. FTC DATA BROKERS REPORT, *supra* note 323, at 11-14 (concluding that data brokers collect data from three categories of sources: government sources, other publicly available sources, and commercial sources).

325. *Id.* at ii.

326. *Id.*

327. *Id.* at 23-31 (detailing the various marketing products offered by data brokers).

328. *Id.* at 32.

329. *Id.*

330. *Id.* at 34.

331. *Id.* (listing the particular types of information available to users through a people search).

332. *Id.* at 46-47.

risks for consumers.[333] They piece together a wealth of personal information from numerous sources to create a "detailed composite of the consumer's life," and they do so without the consumer's knowledge.[334] When they use this information to design marketing products, they group consumers into different categories—including categories that track ethnicity and income level—or assign them different "scores" based on their personal information.[335] These groupings dictate what advertisements consumers see, which can in turn impact which products they buy and what services they receive.[336] When data brokers use their troves of personal information to create people-search products, they could be "facilitat[ing] harassment, or even stalking, and may expose domestic violence victims, law enforcement officers, prosecutors, public officials, or other individuals to retaliation or other harm."[337] And, regardless of how they use the data, storing such large quantities of personal information inherently carries privacy risks attendant to a breach.[338] This is a fact that approximately 250 Mainers learned first-hand during the ChoicePoint data breach that led the state to enact its breach notification law.

Two states have enacted laws governing data brokers in response to these privacy concerns. Vermont was the first state to do so when, in 2017, it enacted legislation creating a data broker registry.[339] Data brokers are required to annually register with the Vermont Secretary of State, to provide the company's contact information, and to provide information about whether and how a consumer can opt-out from the collection or sale of personal information.[340] The Secretary of State then publishes this information in a publicly available, online database so that anyone can contact the data broker.[341] Importantly, the data broker registry is only a transparency measure. It does not create a right to opt-out from the collection or sale of personal information; Vermont law only requires data brokers to be transparent about whether consumers can opt-out, what activity they can opt-out of (e.g., collection or sales), and what they need to do to opt-out.[342]

---

333. The FTC's conclusion that data brokers' practices result in intrusions to consumers' privacy is shared by consumers themselves. The results of an empirical study published in 2017 show that consumers are deeply uncomfortable with data-brokers accessing their personal information, even when that information comes from a public source. *See* Kirsten Martin & Helen Nissenbaum, *Privacy Interests in Public Records: An Empirical Investigation*, 31 HARV. J.L. & TECH. 111, 140 (2017) ("Accessing [public record] information through the use of a data broker is consistently perceived as inappropriate, even when the type of information accessed and the receiver of the information are judged to be appropriate.").

334. FTC DATA BROKERS REPORT, *supra* note 323, at 46.

335. *Id.* at 47-48 (noting data-brokers' scoring system and listing groups such as "'Urban Scramble' and 'Mobile Mixers,' both of which include a high concentration of Latinos and African Americans with low incomes").

336. *See id.* at 48 (noting that a low score could result in a consumer being "limited to ads for subprime credit or receiving different levels of service from companies").

337. *Id.*

338. *Id.* at 48-49 ("[I]dentity thieves and other unscrupulous actors may be attracted to the collection of consumer profiles that would give them a clear picture of consumers' habits over time, thereby enabling them to predict passwords, challenge questions, or other authentication credentials.").

339. *See* VT. STAT. ANN. tit. 9, § 2446 (2019) (creating a data broker registry).

340. *Id.* at § 2446(a).

341. *See* Vermont Data Broker Registry, https://bizfilings.vermont.gov/online/DatabrokerInquire/ [https://perma.cc/5FPF-LW54] (last visited Apr. 11, 2021).

342. VT. STAT. ANN. § 2446(a)(3)(B)(i)-(iii).

In addition to the registration requirement, the Vermont law imposes affirmative information-security obligations on data brokers and creates a private right of action for violations of the security requirements.[343] The law also prohibits the acquisition of brokered personal information through fraudulent means, for purposes of stalking or harassment, for purposes of discriminating, or for committing fraud.[344] Consumers have a private right of action to enforce these prohibitions.[345]

More recently, California amended the CCPA to create a data broker registry.[346] The registry requires data brokers to list: (a) their name and contact information; and (b) "[a]ny additional information or explanation the data broker chooses to provide concerning its data collection practices."[347] The amendment does not create any new rights for consumers, though the CCPA already provides them the right to opt-out from the sale of their personal information.[348]

Maine should adopt a law similar to Vermont's and California's and require data brokers to annually register with the Secretary of State. Establishing a registry is an important transparency measure. Since data brokers collect information from third-party sources, consumers need a registry to know which companies to contact about opting out of the collection or sale of their personal information.

Other desirable features of a Maine data broker law depend on whether the state also enacts a general consumer privacy law, and on what rights and obligations that law respectively creates for consumers and businesses. Whether located in a general consumer privacy law or a specific data broker law, the state should ensure that residents have the right to know what personal information data brokers collect and sell.[349] Maine law could also empower residents to opt-out from data brokers building profiles about them for marketing purposes, from data brokers selling their personal information, and from data brokers disclosing their compiled information to the public in people-search products.[350] This latter right—the right to opt-out from being listed in people-search products—is particularly important for victims of cyber-harassment and stalking that the legislature has repeatedly acted to protect.

---

343. *See id.* § 2447 (detailing the security requirements and stating that "[a] person who violates a provision of this section commits an unfair and deceptive act in commerce in violation" of Vermont's consumer protection laws).

344. *See id.* § 2431.

345. *Id.* § 2431(b)(1).

346. *See* CAL. CIV. CODE §§ 1798.99.80–.88 (West 2020).

347. *Id.*

348. *See supra* Section (II)(A)(2) (discussing the individual rights created by the CCPA).

349. This recommendation aligns with the FTC's recommendation that Congress consider legislation requiring data brokers to give consumers access to their data. *See* FTC DATA BROKERS REPORT, supra note 323, at 50.

350. The FTC report also recommended that consumers be allowed to opt-out from having their data shared for marketing purposes and from being listed in "people search" results. *Id.* at 50, 54. The FTC recommends giving consumers other rights as well, including a right to correct inaccurate information contained in a "people search" listing. *Id.* at 54. The FTC recommendations regarding risk mitigation products are more circumscribed, focusing on increasing transparency rather than vesting consumers with opt-out rights. *Id.* at 53-54. Data brokers' use of personal information to create risk mitigation products present less privacy risks and pose greater benefits to consumers than do the other ways in which data brokers use personal information. In balancing these risks and benefits, providing consumers a right to opt-out from data brokers' use of publicly available information for risk mitigation products is likely not necessary at this time.

Finally, Maine could create a universal opt-out list, much like the National Do Not Call Registry.[351] Creating such a list would allow residents to exercise their opt-out rights for all data brokers at once, rather than having to navigate the opt-out process for each broker individually.

The Maine Information and Analysis Center ("MIAC"): The MIAC is a law enforcement information-sharing center established by executive order and operated jointly by the Maine Emergency Management Agency and the Maine State Police.[352] Known as a "fusion center," the MIAC is one cog in a national network of information-sharing centers established in the wake of the 9/11 attacks to improve the nation's intelligence-sharing practices.[353] Following that tragedy, "policymakers argued that government agencies could have prevented the attacks if they had 'connected the dots' by synthesizing and analyzing available information."[354] The creation of fusion centers to collect and share information between local, state, federal, and private-sector sources was a response to this perceived shortcoming.[355]

In the two decades since 9/11, fusion centers have become the target of frequent criticism regarding both their effectiveness as an intelligence tool and their intrusions on individual liberties. Critics assert that the increase in digital information sharing fostered by fusion centers does not, "actually lead[] to more actionable intelligence than it impedes."[356] The glut of information can instead make it difficult for analysts to distinguish relevant from irrelevant information, and accurate leads from inaccurate leads, amounting to a massive waste of valuable time and resources.[357] Indeed, a U.S. Senate Committee on Homeland Security and Governmental Affairs investigation failed to identify a single instance where a fusion center helped to identify a terrorist threat or to disrupt an active terrorist plot.[358]

---

351. Fed. Trade Comm'n, *National Do Not Call Registry*, https://donotcall.gov [https://perma.cc/9B4P-S7AQ](last visited Apr. 11, 2021).

352. Me. Exec. Order No. 24 FY 06/07 (Dec. 8, 2006) ("An Order Establishing the Maine Intelligence Analysis Center"), https://www.maine.gov/tools/whatsnew/index.php?topic=Gov_Executive_Orders&id=28092&v=Article [https://perma.cc/3CGK-YYBS] (last visited Apr. 11, 2021).

353. *See, e.g.*, Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262, 264 (2013) ("Since 9/11, a surveillance state has been in development, accomplished in part by a network of fusion centers through which government agents and private-sector representatives 'collect and share' information and intelligence.").

354. Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1448 (2011).

355. *Id.*

356. *Id.* at 1456.

357. *See id.* at 1457 ("Analytical tools produce many false leads, draining scarce resources away from more effective crime-fighting endeavors. Amidst the false positives, analysts may find it difficult to find relevant information. They also spend valuable time investigating innocent individuals.").

358. U.S. SENATE PERMANENT SUBCOMM. ON INVESTIGATIONS, COMM. ON HOMELAND SEC. AND GOVERNMENTAL AFFS., FED. SUPPORT FOR AN INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS 2 (Oct. 3, 2012), https://www.hsgac.senate.gov/imo/media/doc/10-3-2012%20PSI%20STAFF%20REPORT%20re%20FUSION%20CENTERS.2.pdf [https://perma.cc/2NVX-NRDS]; Brendan McQuade, *Investigate and Shut Down the Maine Information and Analysis Center,* BANGOR DAILY NEWS (June 13, 2020), https://bangordailynews.com/2020/06/13/opinion/contributors/investigate-and-shut-down-the-maine-information-and-analysis-center/ [https://perma.cc/EHX5-DHZU] (quoting the U.S. Senate Committee investigation in support of the proposition that fusion centers are a "failed policy"); s*ee also* Citron & Pasquale, *supra* note 354, at 1456 ("Although fusion centers have

From the civil liberties perspective, three related factors have spurred calls for reform. First, the scope of fusion centers' missions have drastically expanded from their counter-terrorism origins to encompass all types of general crime prevention.[359] This "mission creep" has led to concerns that the post-9/11 state of emergency originally used to justify the centers' creation has normalized what amounts to a domestic surveillance program.[360] Second, the massive volume of information shared within and between fusion centers has led to privacy concerns common to most any large government database: Is the collection, use, storage, and sharing of information transparent, appropriate, and secure, and what recourse do people have if information about them is inaccurate or incomplete?[361] Third, fusion centers have regularly conducted surveillance on groups engaging in protest activities, leading to concerns that they pose a threat to First Amendment speech and associational rights.[362]

These civil liberty and privacy concerns came to a head in Maine during the summer of 2020. On May 7, 2020, a Maine State Trooper filed a complaint in federal district court alleging that the MIAC retaliated against him for blowing the whistle on the MIAC's illegal surveillance activity.[363] The complaint alleged that the MIAC "completely ignores its own privacy policy, the federal Privacy Act, and that it regularly engages in violations of state law, federal law, and rules of criminal procedure."[364] This alleged misconduct includes collecting, retaining, and sharing data on "individuals associated with lawful public protests . . . ."[365] For example, the MIAC allegedly monitored protests against CMP's transmission line project and

---

contributed to crime-fighting in cases where they assist ongoing investigations, they have generated little valuable intelligence about future threats, crimes, or hazards.").

359. *See* Citron & Pasquale, *supra* note 354, at 1463-65 (describing how fusion centers have expanded from an anti-terrorism focus to an "all hazards, all crimes, all threats" mission).

360. *Id.*; *see also* Danielle Keats Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NOTRE DAME L. REV. 1035, 1051 (2018) (describing how fusion centers' "mission became unmoored from their antiterror beginnings to cover all crimes, threats, and hazards").

361. *See, e.g.*, Citron & Pasquale, *supra* note 354, at 1464-65 (discussing transparency concerns). The collaborative aspect of fusion center—which involves information sharing between different states and between the states and the federal government—may exacerbate the privacy concerns ordinarily attendant to government databases. It can be unclear whether state law (and, which state's law) or federal law supplies the privacy protections for information shared through fusion centers. *See id.* at 1467-69.

362. *See id.* at 1444-46 (describing how the Minnesota fusion center monitored protestors at the 2008 Republican National Convention and how the Maryland fusion center "conducted surveillance of human rights groups, peace activists, and death penalty opponents"); *see also* Alleen Brown et al., *Standing Rock Documents Expose Inner Workings of "Surveillance-Industrial Complex,"* THE INTERCEPT (June 3, 2017, 11:57 AM), https://theintercept.com/2017/06/03/standing-rock-documents-expose-inner-workings-of-surveillance-industrial-complex/ [https://perma.cc/8Q3X-2LJR] (describing the North Dakota fusion center's involvement in surveilling Dakota Access pipeline protesters at Standing Rock); Shawn Musgrave, *Why Was the Austin Counterterrorism Unit Monitoring Vegan Potlucks?*, MUCKROCK (May 7, 2015), https://www.muckrock.com/news/archives/2015/may/07/vegan-potlucks-anime-screenings-counterrorism-unit/ [https://perma.cc/JKZ4-N9QZ] (describing emails released from the Austin, TX fusion center showing that the center monitored animal rights activists).

363. Complaint & Demand for Jury Trial at ¶¶ 13-16, Loder v. Me. Intel. Analysis Ctr., No. 2:20-cv-00157-JDL (D. Me. May 7, 2020).

364. *Id.* at ¶¶ 57, 63.

365. *Id.* ¶59.

shared its information with CMP.[366] The MIAC also allegedly maintains records about gun owners indefinitely, in violation of federal and state law.[367] And, the MIAC allegedly compiled information on individuals connected with a summer camp, Seeds of Peace, which hosts foreign teenagers from international conflict areas.[368]

The second shoe dropped a month later when an online "hactivist" group published a trove of law enforcement documents obtained from servers owned by a website developer called Netsential.[369] The so-called "Blueleaks" hack included numerous documents from the MIAC. Among other issues, these documents revealed that the MIAC was closely monitoring Black Lives Matter ("BLM") protests across the state. The documents included compilations of the times and places of protests, misleading information about an incident that occurred at one protest, and the documents showed that the MIAC had shared unverified anti-BLM information emanating from far right-wing Twitter accounts.[370] The MIAC's monitoring of, and spread of misinformation about, BLM protests suggests a "political nature" to MIAC's surveillance practices.[371] The concern that the MIAC's monitoring of protests has political underpinnings carries particular weight in the context of a movement sparked by police brutality, whose organizers have called for defunding police departments, and who many law enforcement officials see as being anti-police.

These revelations have prompted calls to reform or defund the MIAC. Brendan McQuade, an Assistant Professor of Criminology at the University of Southern Maine and author of a book on fusion centers, has called for the MIAC to be shut down.[372] State Representative Charlotte Warren, the Chair of the House's Criminal Justice Committee, has called for the MIAC to be defunded.[373] And, the editorial

366. *Id.* ¶ 60.

367. *Id.* ¶ 64.

368. *Id.* ¶ 94; *FAQs,* SEEDS OF PEACE, https://www.seedsofpeace.org/faq/ [https://perma.cc/TS6R-2WNX] (last visited Apr. 11, 2021) (describing the camp's mission and programs).

369. *See* Andy Greenberg, *Hack Brief: Anonymous Stole and Leaked a Megatrove of Police Documents*, WIRED , (June 22, 2020) https://www.wired.com/story/blueleaks-anonymous-law-enforcement-hack/ [https://perma.cc/XH6M-HSZY].

370. *See* Megan Gray, *Hack Included Documents from Secretive Maine Police Unit*, PORTLAND PRESS HERALD (June 26, 2020), https://www.pressherald.com/2020/06/26/hack-included-documents-from-secretive-maine-police-unit/ [https://perma.cc/J6L6-V5H6]; Nathan Bernard, *Maine Spy Agency Spread Far-Right Rumors of BLM Protest Violence*, MAINER NEWS (July 7, 2020), https://mainernews.com/maine-spy-agency-spread-far-right-rumors-of-blm-protest-violence/ [https://perma.cc/PNE6-8XF8]; Mike Tipping, *Data Breach Exposes Activities of Maine's Secretive Police Intelligence Agency*, ME. BEACON (June 26, 2020), https://mainebeacon.com/data-breach-exposes-activities-of-maines-secretive-police-intelligence-agency/ [https://perma.cc/XP66-WQU2].

371. Bernard, *supra* note 370 (quoting University of Southern Maine criminology professor Brendan McQuade).

372. McQuade, *supra* note 358; *see also* Letter from Brendan McQuade, Assistant Professor, Univ. S. Me., to Reps. Charlotte Warren, Thom Harnett, Craig Hickman, & Rachel Talbott Ross (June 25, 2020) (on file with author) (encouraging the representatives to investigate the MIAC and to shut it down).

373. Dan Neumann, *Maine's Police Intelligence Center Sent Reports on Activists to Corporations*, ME. BEACON (July 16, 2020), https://mainebeacon.com/maines-police-intelligence-center-sent-reports-on-activists-to-corporations/ [https://perma.cc/V5KX-DR22] (stating that Rep. Warren has called for the MIAC's $700,000 annual budget to be redirected to serve other needs).

boards of the state's two largest newspapers have both called for investigations and reforms for the MIAC.[374]

I add my voice to this chorus. As this Article goes to print, Maine's legislature is considering a bill to defund the MIAC.[375] Given the aforementioned abuses, the legislature should pass this bill and the Governor should sign it into law.[376]

IV. CONCLUSION

In the late 1960s, Maine began developing a body of privacy law to protect its residents from privacy risks posed by the likes of eavesdroppers, harassers, wiretappers, private investigators, and consumer reporting agencies. The state has since expanded upon these foundational privacy protections to account for advances in technology. During the 1990s and early 2000s, Maine criminalized unauthorized computer access, prohibited cyberstalking, expanded the state's criminal invasion of privacy law, enacted a data breach law, prohibited the sale of consumers' cell phone records, and more. In the years since, Maine has enacted targeted reforms aimed at specific privacy intrusions that have emerged during the current era of social media, big data, and machine learning, curtailing the privacy risks caused by ISPs, education technologies, drones, social media in employment, and unauthorized sexual images.

These recent reforms should be viewed as just the beginning of Maine's efforts to protect its residents against the day's privacy threats. Personal information has become a valuable resource that drives a significant portion of the country's economy. As with natural resources like oil, gas, and minerals, the titans of industry have strong financial incentives to gather, process, market, and exploit more and more of the new resource. If this industry continues to be left virtually unchecked, the mass-commoditization of personal information will lead Mainers and other Americans to experience unprecedented harms to their privacy.

This is no longer a case where "technology got a couple of steps ahead of us," as Senator Bartlett remarked while discussing the state's Cellular Telephone Customer Privacy Act.[377] An entire system of economic production has gotten a

---

374. *See* Editorial Board, *Our View: Oversight of Maine State Police 'Fusion Center' Way Overdue*, PORTLAND PRESS HERALD (May 20, 2020), https://www.pressherald.com/2020/05/20/our-view-oversight-for-maine-state-police-fusion-center-way-overdue [https://perma.cc/J5FK-9LAW]; Editorial Board, *Our View: Hearing on Maine Fusion Center Fails to Provide Answers*, PORTLAND PRESS HERALD (June 26, 2020), https://www.pressherald.com/2020/06/26/our-view-hearing-on-fusion-center-fails-to-provide-answers-2/ [https://perma.cc/L3XL-66WK]; Editorial Board, *Legislators Should Continue Scrutiny of MIAC Activity, Budget*, BANGOR DAILY NEWS (July 14, 2020), https://bangordailynews.com/2020/07/14/opinion/editorials/legislators-should-continue-scrutiny-of-miac-activity-budget/ [https://perma.cc/7SS7-528D].

375. An Act to End the Maine Information and Analysis Center Program, L.D. 1278 (130th Legis. 2021).

376. In the event the Legislature decides not to defund the MIAC, I note that it is unclear what existing legal authority the MIAC has to conduct intelligence analysis outside of the counter-terrorism context. The executive order creating the MIAC refers only to "Homeland Security intelligence information" and declares that the overall goal of the MIAC is "securing Maine's citizens and infrastructure from the threat of terrorism . . . ." Me. Exec. Order No. 24 FT 06/07 (Dec. 8, 2006). Conspicuously absent from the executive order is any grant of authority to conduct general crime-prevention operations or to surveil domestic protest movements with no links to terrorism.

377. *See* remarks of Sen. Bartlett, *supra* note 112.

couple steps ahead of us. Maine should correct this lag by enacting a general consumer privacy law with the features described in this Article. Most importantly, the law should endow a state agency with rulemaking authority over consumer privacy issues such that the state can adapt its laws to changing industry practices and new technologies. Maine should also continue to regulate specific threats posed by emerging technologies. Facial recognition technology, biometric information, smart-home devices, data brokers, and the MIAC all pose privacy threats that the state should address through specific regulation, legislation, or executive action.

To be sure, this era's privacy risks are national—and indeed global—in scope; they require national and international solutions. But Maine should not leave its residents' privacy unguarded while waiting patiently for a federal response that may not come or may be too little, too late.