St. John's Law Review

Volume 92, Summer 2018, Number 2 Article 4

Tactful Inattention: Erving Goffman, Privacy in the Digital Age, and the Virtue of Averting One's Eyes

Elizabeth De Armond

TACTFUL INATTENTION: ERVING GOFFMAN, PRIVACY IN THE DIGITAL AGE, AND THE VIRTUE OF AVERTING ONE'S EYES

ELIZABETH DE ARMOND[†]

Finders, keepers
Losers, weepers[1]

Mind your own beeswax[2]

INTRODUCTION

According to the sociologist Erving Goffman, we each need a backstage in which we "can relax; [we] can drop [our] front, forgo speaking [our] lines and step out of character."[3] That is, we need a place to free ourselves from the "façade of performance" that being in front of others can impose.[4] Shielding one's backstage from outsiders has become much harder. Developments in information technology have made accessible all sorts of "backstage" areas, including our social activities with family and friends, our financial choices and commitments, and our purchasing preferences, among heaps of others. With all the information swirling around us, we may have to innovate our approaches to protecting privacy.

Rather than feasting on any and all data we can find, perhaps, we could occasionally avert our eyes from information that's not our own. "Tactful inattention,"[5] coined by Goffman,

---

[†] Professor, Legal Research and Writing and Director of Legal Writing, Chicago-Kent College of Law, Illinois Institute of Technology.

[1] Old English adage.

[2] American saying, attributed by some to colonial America. *See* STEVEN D. PRICE, ENDANGERED PHRASES: INTRIGUING IDIOMS DANGEROUSLY CLOSE TO EXTINCTION 144 (2011).

[3] ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE 70 (1959) [hereinafter GOFFMAN, THE PRESENTATION].

[4] Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIAMI L. REV. 559, 570 (2015) (citing GOFFMAN, THE PRESENTATION, *supra* note 3, at 112).

[5] Goffman also sometimes referred to it as "civil inattention." *See, e.g.*, ERVING GOFFMAN, BEHAVIOR IN PUBLIC PLACES: NOTES ON THE SOCIAL ORGANIZATION OF GATHERINGS 84 (1963). Subsequently, Professor Anita Allen described a similar

describes the appropriate response of an outsider who makes an "inopportune intrusion[]" into a region where insiders have "patently been witnessed in activity that is quite incompatible with the impression that they are, for wider social reasons, in a position to maintain to the intruder."[6] An outsider should adopt this tactful inattention response when that outsider gained access to the insider's area notwithstanding the insider's intentions to keep the region, the "backstage," curtained off, at least from that particular intruder.[7] The insider and the outsider share the burden—the insider must take steps to create a bounded backstage, and, correspondingly, the outsider must observe those boundaries.

With the phrase "tactful inattention," Goffman captured the socially salutary response to the undue access to someone's backstage; it is a sort of averting one's eyes, as one might do, for instance, in a locker room or a gym. Information may be available to you, but you should not scrutinize it or use it to your own advantage.

However, in contrast to the tactful inattention paradigm, many laws intended to protect privacy protect only "secret" information, and largely prohibit the disclosure, rather than the use of the information. Under this paradigm, which Professor Daniel Solove labels the "secrecy paradigm,"[8] to prevent others from using information they have acquired about you for evaluating you, you must keep the information entirely under wraps. This can be thought of as the "finders-keepers" paradigm. Privacy laws that adopt the secrecy paradigm assume that the way to protect individual privacy is for the individual to entomb the information. However, the secrecy paradigm is at odds with advances in information technology that have crippled our ability to keep information secret. We dribble data crumbs everywhere we go, leaving the possibility that the only backstage area

---

concept of "virtuous inattention." *See* Anita Allen, *Privacy Law: Positive Theory and Normative Practice*, 126 HARV. L. REV. F. 241, 243–44 (2013).

[6] GOFFMAN, THE PRESENTATION, *supra* note 3, at 132.

[7] *See id.* at 132–35.

[8] *See, e.g.*, DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 42–44 (2004); Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 MINN. L. REV. 1137, 1140–41 (2002) ("[T]he 'secrecy paradigm[]' understands privacy as depending upon whether information is secret or non-secret. The secrecy paradigm fails to account for the realities of the Information Age, where information is rarely completely confidential.").

remaining to any of us is the interior of our own heads.[9] The ease with which these crumbs can be mapped, linked, copied, and shared by electronic means has exponentially increased the accessibility of personal information, and correspondingly crippled the efficacy of the secrecy paradigm.

As barriers to accessibility of information have dissolved, the secrecy paradigm leads to a game of cat and mouse, with the winner taking the position that discovery yields all spoils. To dislodge an item of information is to destroy any privacy entitlement. This is a "gotcha" paradigm for privacy, whereby revealing any information, even unintentionally, risks making it available for all to see—and use. The entire burden for protecting privacy rests on the target.

Given our human, sociological need for a backstage, though, this secrecy paradigm rewards those who can use technology to shine a spotlight into the darkest niche of every closet, while enfeebling individual privacy and the maintenance of backstage areas that might allow us to avoid "discrediting,"[10] an unexpected and unsought change in status.[11] To that point, humans may well be motivated to discredit. Goffman emphasizes that by nature, humans are eager to "pounce on chinks in [our] symbolic armour in order to discredit [our] pretensions."[12]

This Article suggests that we would benefit if we would protect privacy by sometimes requiring tactful inattention by potential users rather than total secrecy by the target. That is, some legal privacy protections should stop emphasizing secrecy and instead emphasize the appropriate uses of personally identifiable and often sensitive information by gelling tactful inattention into legal standards. Culturally, such an expansion may be difficult, as we tend to a "finders-keepers" attitude towards data. However, given technology's ability to dissolve routine barriers, if we require others to leave some information

---

[9] As neuroscience develops, who knows how long it will be before we will read brain waves as easily as *The New York Times*? *See* Joëlle Anne Moreno, *The Future of Neuroimaged Lie Detection and the Law*, 42 AKRON L. REV. 717, 717–22 (2009) (describing some recent developments in cognitive neuroscience research).

[10] GOFFMAN, THE PRESENTATION, *supra* note 3, at 7. Goffman emphasized the role of "tact," explaining that "few impressions could survive if those who received the impression did not exert tact in their reception of it." *Id.* at 7.

[11] Erving Goffman, *Embarrassment and Social Organization*, 62 AM. J. OF SOC. 264, 268 (1956).

[12] GOFFMAN, THE PRESENTATION, *supra* note 3, at 38.

out of some equations, we may be able to retain the personal flourishing that privacy promotes, without unduly impairing the information needs of others.

Not only has the tactful inattention paradigm already existed in some traditional areas of law, but it also has occurred in some new laws in specific areas of recent concern. Part I discusses the benefits to flourishing that privacy provides, both individually and within relationships. Part II describes the development of the tactful inattention paradigm in various areas of law. Part III suggests two specific areas that might benefit from a paradigm of tactful inattention: the use of certain behavioral information by employers to screen applicants and employees, and the use of similar information by political campaigns and vendors to target behavioral advertising and for vendors, micro-target pricing. Finally, Part IV describes the benefits of a tactful inattention approach to privacy in the digital age.

I. THE HUMAN NEED FOR A BACKSTAGE TO FLOURISH

A. Philosophers on Privacy—Goffman and Others

To thrive and flourish—to achieve Aristotle's "eudaemonia"[13]—we need a "backstage" on which to try on various roles, and test and assess our reactions to ourselves, others, and events. Furthermore, we need a sheltered area not only for our own thoughts, but for some of our relations with others. These relationships benefit not only ourselves, but also society as a whole. To mark the boundaries of these backstage areas, we use social rules and conventions that protect dignity.[14]

---

[13] *See Eudemonic*, THE OXFORD ENGLISH DICTIONARY (2d ed. 1989) (defining "eudemonic" as being "[c]onducive to happiness"); *see also* K. Craig Welkener, *Possible but Not Easy: Living the Virtues and Defending the Guilty*, 26 GEO. J. LEGAL ETHICS 1083, 1093 (2013) ("Though commentators explain that *eudemonia* is impossible to translate adequately into English, its central meaning can be expressed as the good life, a state of wholeness, or flourishing."); ARISTOTLE, NICOMACHEAN ETHICS 307 (Martin Ostwald trans., Prentice Hall, Inc., 1999) (c. 384 B.C.E.) (emphasis in original) (defining "*eudaimon*" to mean "[H]APPY, usually in the sense of a happiness attained by man through his own efforts").

[14] Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 962 (1989); *see also* Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 971 (1964) (describing Warren and Brandeis's "principle of 'inviolate personality' to posit the individual's independence, dignity and integrity").

1. The Backstage for Our Own Thoughts

To have a backstage promotes personhood[15] and autonomy.[16] To protect personhood is to allow ourselves and others to develop and maintain the "inviolate personality" of Warren and Brandeis fame.[17]

When one is completely deprived of a backstage, such as in a prison or an asylum, we suffer what Erving Goffman describes as an effect of "contaminative exposure."[18] Robert Gerstein has emphasized that such "contaminative exposure" hampers autonomy: "It is clear that anyone who intrudes uninvited on the intimacy of another person interferes with his autonomy in a very serious way."[19]

Thus, to preserve autonomy, we need some sort of partition that shields us from exposure. The scholars Georg Simmel, Erving Goffman, Robert Post, and Alan Westin all speak of a buffer around individuals that protects their privacy.[20] For Simmel, the buffer is one of "reciprocal reserve and indifference,"[21] which places an "ideal sphere [that] lies around every human being";[22] for Goffman, it is an "information

---

[15] Paul Freund defined "personhood" to mean "those attributes of an individual which are irreducible in his selfhood." Paul A. Freund, Address, 52 A.L.I. PROC. 574 (1975); *see also* Jessica L. Roberts, *Protecting Privacy to Prevent Discrimination*, 56 WM. & MARY L. REV. 2097, 2106 (2015) ("Protecting privacy allows us to more freely construct our identities and negotiate our social interactions."); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1116 (2002).

[16] *See, e.g.*, Roberts, *supra* note 15, at 2105–06 ("Insofar as privacy is construed as a matter of control, its primary underlying norm is autonomy."); Robert S. Gerstein, *Intimacy and Privacy*, 89 ETHICS 76, 78 (1978).

[17] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205 (1890). The phrase has been criticized as being too imprecise. *See* David Rosen & Aaron Santesso, *Inviolate Personality and the Literary Roots of the Right to Privacy*, 23 LAW & LITERATURE 1, 6 (2011); *see also* Solove, *supra* note 15, at 1118 (criticizing the theory of privacy as personhood for failing to adequately define "personhood").

[18] ERVING GOFFMAN, ASYLUMS: ESSAYS ON THE SOCIAL SITUATION OF MENTAL PATIENTS AND OTHER INMATES 23 (1961) [hereinafter GOFFMAN, ASYLUMS]. Goffman describes the process of admission to such an institution, emphasizing the accumulation of losses of privacy, from having one's body and possessions physically searched, to sleeping in a communal space, using doorless toilets, and suffering ceaseless surveillance. *Id.* at 16–25.

[19] Gerstein, *supra* note 16, at 76, 78, 80 (1978) (citing GOFFMAN, ASYLUMS, *supra* note 18).

[20] *See infra* notes 21–24 and accompanying text.

[21] GEORG SIMMEL, THE SOCIOLOGY OF GEORG SIMMEL 418 (KURT H. WOLFF ED. & TRANS., 1951).

[22] *Id.* at 321.

preserve[]";[23] for Post, the buffer is a "sacred precinct[]";[24] for Westin, such a buffer is a reserve, a state of privacy that exists as "a psychological barrier against unwanted intrusion."[25]

This buffer protects our dignity and our personhood.[26] Jeffrey Reiman argues that "privacy is necessary to the creation of *selves* out of human beings, since a self is at least in part a human being who regards his existence—his thoughts, his body, his actions—as his *own*."[27] Similarly, Stefano Scoglio emphasizes the value of "interiority," "the ability to be self-reflecting and critical without reflecting whims imposed by mass-market culture."[28]

When others breach the rules that protect these buffers, they "damage a person by discrediting his identity and injuring his personality."[29] To uphold these rules through, for example, legal devices like privacy torts, "simultaneously uphold[s] social norms and redress[es] 'injury to personality.' "[30]

---

[23] ERVING GOFFMAN, *The Territories of the Self*, *in* RELATIONS IN PUBLIC: MICROSTUDIES OF THE PUBLIC ORDER 38–39 (1971) [hereinafter GOFFMAN, *The Territories of the Self*] (identifying "[t]he set of facts about [one]self to which an individual expects to control access while in the presence of others").

[24] Post, *supra* note 14, at 960 (quoting Griswold v. Connecticut, 381 U.S. 479, 485 (1965)).

[25] ALAN F. WESTIN, PRIVACY AND FREEDOM 32 (1967). Reserve is one of the four states of privacy that Alan Westin identifies, along with solitude, anonymity, and intimacy. *Id.* at 31; *see also* Alan F. Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's Part I—The Current Impact of Surveillance on Privacy*, 66 COLUM. L. REV. 1003, 1022 (1966) (describing reserve as the " 'mental distance' to protect the personality," that "takes place in every sort of relationship under the rules of social etiquette").

[26] Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, 6 PHIL. & PUB. AFF. 26, 37 (1976) ("[P]rivacy is fundamentally connected to personhood."); *see also* Julie E. Cohen, *What Privacy Is for*, 126 HARV. L. REV. 1904, 1906, 1911 (2013) ("Privacy is shorthand for breathing room to engage in the processes of boundary management that enable and constitute self-development," and "is one of the resources that situated subjects require to flourish.").

[27] Reiman, *supra* note 26, at 39 (emphasis in original).

[28] Daniel E. Newman, *European Union and United States Personal Information Privacy and Human Rights Philosophy—Is There a Match?*, 22 TEMP. INT'L & COMP. L.J. 307, 315 (2008) (citing STEFANO SCOGLIO, TRANSFORMING PRIVACY: A TRANSPARENT PHILOSOPHY OF RIGHTS 2 (1998)).

[29] Post, *supra* note 14, at 963. Post states that "[b]y following these rules, individuals not only confirm the social order in which they live, but they also establish and affirm 'ritual' and 'sacred' aspects of their own and others' identities." *Id.* at 962.

[30] *Id.* at 963.

2. The Backstage for Our Relationships

While we need privacy to preserve the solitude of our relationship with ourselves, privacy is also important to our relationships with others; Professor Charles Fried argues that without privacy, relations of "respect, love, friendship and trust" become impossible.[31] He, too, rests these relations on the concept of personality.[32] Like Goffman, Fried invokes the concept of respect for others.[33] He rejects the privacy-as-secrecy paradigm, characterizing privacy as "the control we have over information about ourselves."[34] Fried argues that privacy permits us to "modulate" friendships,[35] and to learn to "express our humanity" by learning to accord trust.[36]

We can find examples of judicial recognition of the need for privacy to protect and nourish such intimate relationships. For instance, in *Hamberger v. Eastman*, a licentious landlord stealthily installed a secret recording device in the bedroom of the home he had rented to the plaintiffs, a married couple.[37] The landlord wired the device to transmit into his own home.[38] When the plaintiffs uncovered the recorder, they sued the landlord for invasion of privacy. The landlord argued that the New Hampshire Supreme Court should dismiss the couple's invasion of privacy claim because they did not allege that anyone actually listened to or overheard any sounds from the bedroom.[39] However, the court rejected that argument, concluding that the installation of the eavesdropping device was an "injury to personality."[40] The court compared the conduct to that of a "Peeping Tom," and quoted Pound's Jurisprudence to describe

---

[31] Charles Fried, *Privacy*, 77 YALE L.J. 475, 477 (1968).

[32] *Id.* at 478.

[33] *Id.* at 479. Fried describes respect as a correlative to morality, something we are obligated to demonstrate to one another simply by virtue of being persons. *Id.*

[34] *Id.* at 482 (emphasis in original). Furthermore, he sees privacy as a feature of liberty. *Id.* at 483.

[35] *Id.* at 485.

[36] *Id.* at 486. He acknowledges, though, that our privacy can be only "relative and qualified." *Id.*

[37] 206 A.2d 239, 239–40 (N.H. 1964).

[38] *Id.*

[39] *Id.* at 242.

[40] *Id.*

the injury as one that "may produce suffering more acute than that produced by a mere bodily injury"[41] within the married plaintiffs' intimate relationship.

Professor Post linked the *Hamberger* court's respect for the couple's intruded-upon space to the language of the United States Supreme Court in *Griswold v. Connecticut*: the marital space was a " 'sacred precinct[]' . . . into which it is plainly highly offensive to intrude."[42] This sacred precinct did not lie solely within the boundaries of either the husband or the wife's personality, but rather within the space those personalities shared.[43]

A backstage for our relationships allows us to have room to develop what James Rachels describes as different patterns of behavior for different relationships.[44] Privacy allows us to control "who has access to us," and without that control "we cannot control the patterns of behavior we need to adopt . . . or the kinds of relations with other people that we will have."[45]

Accordingly, by protecting privacy, we create space for intimate relationships to flourish, contributing to their participants' eudemonia.

3. Preservation of Backstages Through Rules of Civility

So if our personhoods and our relationships with others need backstage areas to thrive, how do we define those areas and then protect them? The secrecy paradigm would have us erect impermeable domes over them, but doing so may choke our flourishing, both of ourselves and of our chosen relationships. In that case, we might well have to go "off the grid" completely to avoid inadvertently dribbling data that others could use to discredit and harm us, both individually and as members of relationships. In contrast, under the tactful inattention

---

[41] *Id.* (quoting III POUND, JURISPRUDENCE 58 (1959)). Post critiques this aspect of the *Hamberger* opinion because it places "an intense and narrow focus on the actual mental suffering of specific individuals." Post, *supra* note 14, at 960.

[42] *Id.* at 960 (quoting Griswold v. Connecticut, 381 U.S. 479, 485 (1965)).

[43] *Griswold*, 381 U.S. at 485–86.

[44] James Rachels, *Why Privacy Is Important*, 4 PHIL. & PUB. AFF. 323, 327 (1975). Rachels states these different patterns of behavior "are an important part of what makes the different relationships what they are." *Id.*; *see also* Roberts, *supra* note 15, at 2107 (footnotes omitted) ("[P]rivacy is essential to our relationships. What we reveal to an employer will differ from what we reveal to a family member, which will likewise differ from what we reveal to a lover.").

[45] Rachels, *supra* note 44, at 331.

paradigm, we may justifiably expect that others will avert their eyes from information in which they do not have a sufficient interest.[46]

Law is an "essential element" of privacy,[47] and accordingly necessary to fully obtain the benefits of personal flourishing and fulfilling relationships, along with the societal advantages that flow from both. As explained above,[48] a number of privacy scholars have described a buffer around individuals, and around those engaged in intimate relationships with one another, that helps them flourish and that they are entitled to keep shielded. How can law map and preserve such buffers, given the omniscient availability of data and the avaricious appetites of others for it?

In terms of the buffer's dimensions, many privacy scholars have referred to some set of rules, or conventions, that should set the boundaries of the areas to which others should give tactful inattention. In the past, this buffer, these "information preserves,"[49] often had a geographical aspect. For instance, to illustrate territories of reserve, Professor Post relies on the public disclosure case of *Huskey v. N.B.C.*, in which a prisoner who was filmed while in the prison's exercise cage successfully stated a claim for invasion of privacy against the television network N.B.C. for that filming.[50] In this case, the prisoner's "information preserve" was the "expectation . . . that the only ones able to see him would be persons 'to whom he might be exposed as a necessary result of his incarceration.' "[51] The court rejected the television network's argument that the fact that the plaintiff could have been seen by others within the prison meant that he could not be "secluded" for purposes of the tort.[52] The prisoner

---

[46] For Goffman, tactful inattention, which he also called "civil inattention," "gives to another enough visual notice to demonstrate that one appreciates that the other is present . . . while at the next moment withdrawing one's attention . . . so as to express that he does not constitute a target of special curiosity or design." ERVING GOFFMAN, BEHAVIOR IN PUBLIC PLACES: NOTES ON THE SOCIAL ORGANIZATION OF GATHERINGS 84 (1963).

[47] Fried, *supra* note 31, at 493.

[48] *See supra* text accompanying notes 14–47.

[49] GOFFMAN, *The Territories of the Self*, *supra* note 23, at 38–39.

[50] 632 F. Supp. 1282, 1285 (N.D. Ill. 1986).

[51] *Id.* at 1285.

[52] *Id.* at 1287. Judge Shadur also noted that "one paradigm case of the tort is the Peeping Tom." *Id.* at 1288.

had been in an area generally outside of the gaze of visitors, one in which he could feel "justifiably secluded from the outside world."[53]

As Post construes it, the court allowed the "actual customs and usages of the exercise cage," and not the " 'objective' facts of visibility, secrecy, anonymity, and solitude," to define the boundaries of the territory in which the prisoner could "legally claim the right to undisturbed 'seclusion.' "[54] Construing the boundaries this way helped to redistribute the power to discredit, protecting dignity and autonomy.

In a similar vein, Fried identifies "convention" as defining private areas.[55] To preserve these conventions is to justifiably demand that others give them tactful inattention. Meanwhile, the *Hamberger* decision referred to "rules of decency recognized by the reasonable man."[56] As mentioned above, Professor Post, for his part, describes these as rules of civility, which can help define the boundaries of tactful inattention.[57]

Jeffrey Reiman also identifies space-framing rules, though not as rules of civility but rather as a "social practice."[58] He refers obliquely to the boundaries of civility rules by describing privacy in relation to the act of "refraining," which is another way of saying "inattending." According to Reiman, privacy is a "complex of behaviors that stretches from refraining from asking questions about what is none of one's business to refraining from looking into open windows one passes on the street, from refraining from entering a locked door without knocking."[59] "Privacy is a social ritual by means of which an individual's moral title to his existence is conferred."[60] As examples of these rules embodied in law, Post identifies the paired privacy torts of intrusion upon seclusion and public disclosure of private facts as "safeguard[ing] rules of civility."[61] These torts thereby protect individuals from "the dignitary harm [that] plaintiffs suffer as a

---

[53] *Id.*

[54] *See* Post, *supra* note 14, at 972.

[55] Fried, *supra* note 31, at 487.

[56] Post, *supra* note 14, at 963.

[57] *Id.* at 984. (citing ERVING GOFFMAN, *The Nature of Deference and Demeanor*, *in* INTERACTION RITUAL: ESSAYS ON FACE-TO-FACE BEHAVIOR 47 (1967)).

[58] Reiman, *supra* note 26, at 38.

[59] *Id.* at 38–39.

[60] *Id.* at 39.

[61] Post, *supra* note 14, at 959.

result of having been treated disrespectfully,"[62] much the same way that Fried discusses the right of people to be treated with respect.[63]

Privacy rules support personality development by encouraging what Professor Anita Allen calls "virtuous inattention," promoting a "moral virtue" of "[a] balance of inattention to others' personal lives and attention to one's own . . . ."[64]

B. The Secrecy Paradigm's Impairment of the Backstage

The secrecy paradigm restricts information by focusing on nondisclosure, seeking to maintain privacy by "hiding" information.[65] Sometimes the burden is on the person to whom the information pertains. Other times, the burden to keep information secret is not on the target—the person to whom the information pertains—but on a third party who possesses the information. A classic secrecy paradigm presents itself in the Fourth Amendment's third-party doctrine, which provides that a party usually loses all Fourth Amendment expectations of privacy in any information disclosed to a third party. To disclose to one is to disclose to all, and most especially, to the government.[66]

The Supreme Court created the third-party doctrine in *United States v. Miller*, where it held that the defendant, a bank depositor, had no protectable interest under the Fourth Amendment in his bank records, subpoenaed by the Treasury Department.[67] The Court reasoned that the subpoenaed documents "[were] not [his] 'private papers' " because they "contain[ed] only information voluntarily conveyed to the

---

[62] *Id.* at 967. Post distinguishes this sort of harm from the "contingent psychological injuries that plaintiffs may suffer as a result of the violation of civility rules." *Id.* at 966.

[63] Fried, *supra* note 31, at 478.

[64] Allen, *supra* note 5, at 244 ("Inattention to others' personal lives may also be a qualitative benefit to civil society.").

[65] *See supra* Part I and accompanying footnotes.

[66] *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1036 (2010). *But see* United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) (stating that "the mere ability of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy" and holding that an email recipient could retain a constitutionally-recognized expectation of privacy in email).

[67] 425 U.S. 435, 436–37 (1976).

banks."[68] Accordingly, "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[69]

The Court developed the doctrine more fully in *Smith v. Maryland*,[70] in which the petitioner was a robber caught after he harassed his victim by calling her from his home phone.[71] Using the victim's description of the robber and his car, the police investigating the calls were able to trace the robber's license plate number, and then his home address.[72] Without a warrant, the police had the telephone company install a pen register to record the numbers dialed from the thief's home, which recorded a call to the victim.[73] On the basis of that evidence, the police sought a warrant to search the thief's home and found evidence that led to his arrest and conviction.[74] The thief challenged the denial of his motion to suppress the evidence from the warrantless pen register, arguing that he had an expectation of privacy in the numbers that he dialed.[75] However, the Court ruled that any such expectation was unreasonable because he knew that he was disclosing the dialed numbers to the telephone company, who needed the numbers to connect his call and to bill him.[76] In other words, he "voluntarily" turned over that information to a third party—the telephone company—and thereby lost any expectation of privacy in them.[77]

The third-party doctrine has received harsh criticism for its conception of privacy, one "that views Fourth Amendment privacy as constituting a form of total secrecy."[78] Its application

---

[68] *Id.* at 441–42.
[69] *Id.* at 443.
[70] 442 U.S. 735, 735 (1979).
[71] *Id.* at 737.
[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] *Id.* at 737–38.
[76] *Id.* at 742.
[77] *Id.* at 744.
[78] Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1136 (2002). Professor Henderson states that:

> The third party doctrine is objectionable even if limited as recommended. First, it treats privacy as an indivisible commodity—once information is given to any one party for any one purpose, it is treated as if it were given to every person for any possible purpose as far as the Fourth Amendment is concerned.

Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 546 (2005). Another

to modern digital data raises specific concerns, as the Supreme Court recognized in 2018 in *Carpenter v. United States*.[79] There, five justices trimmed the reach of *Smith* and *Miller*, concluding that the law enforcement's capture of cell phones' cell-site location information from telecommunications companies is a search that generally requires a warrant under the Fourth Amendment.[80] The Court emphasized the sensitivity of the data: "the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements," but also " 'the privacies of life.' "[81]

While the third-party doctrine would have concluded that the cell-phone user voluntarily released the information to their providers and thereby lost their privacy interests, the *Carpenter* majority firmly rejected that application, reasoning that the doctrine assumes "that an individual has a reduced expectation of privacy in information knowingly shared with another."[82] But even where one shares information, the doctrine must consider "the nature of the particular documents sought."[83] Cell-site location data can provide "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." In contrast, *Smith*'s call logs and *Miller*'s checks conveyed limited information.[84] Furthermore, the doctrine's other rationale, voluntary exposure of the data, did not logically extend to data like cell phone location information because "in no

scholar states that "[t]he theory in *Smith* rests on a fallacy," and compares the government's "snooping" through such third-party information as "smack[ing] of Orwell's Big Brother, protection from which is the essence of the [F]ourth [A]mendment." Brian J. Serr, *Great Expectations of Privacy: A New Model for Fourth Amendment Protection*, 73 MINN. L. REV. 583, 600 (1989); *see also* Marissa A. Lalli, Note, *Spicy Little Conversations: Technology in the Workplace and a Call for a New Cross-Doctrinal Jurisprudence*, 48 AM. CRIM. L. REV. 243, 261 (2011) (identifying "significant backlash from scholars who find it outdated").

[79] 138 S. Ct. 2206 (2018).

[80] *Id.* at 2221.

[81] *Id.* at 2217 (quoting Riley v. California, 134 S. Ct. 2473, 2494–95 (2014)).

[82] *Id.* at 2219.

[83] *Id.*

[84] *Id.* The Court characterized the location data as "present[ing] even greater privacy concerns than [that of] GPS monitoring of a vehicle." *Id.* at 2218. It noted that "[w]hile individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Id.*

meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements."[85]

Nonetheless, the reach of *Carpenter* is narrow for the moment,[86] and the secrecy paradigm continues to animate many laws outside of the Fourth Amendment realm. For instance, the Health Insurance Portability and Accountability Act's[87] Privacy Rule[88] prohibits regulated parties from disclosing individually identifiable health information, and is broadly defined to include just about any health-related information traceable to a particular individual.[89] It represents the secrecy paradigm by requiring identifiable data to be entombed, rather than by requiring others to avert their eyes from the identifying markers.[90] In addition, business associates who receive personally identifiable information are subject to contractual restrictions that bar them from re-disclosing the information under many circumstances.[91]

---

[85] *Id.* at 2220 (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979)).

[86] *Id.* at 2220 ("Our decision today is a narrow one. We do not express a view on matters not before us . . . .").

[87] Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[88] The Privacy Rule, 45 C.F.R. §§ 160.101–161.105, 164.101–164.106, 164.500–164.534 (2013).

[89] 42 U.S.C. § 1320d(6) (2012). The full definition is as follows:

> The term "individually identifiable health information" means any information, including demographic information collected from an individual, that--
>
> (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
>
> (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and--
>
> (i) identifies the individual; or
>
> (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

[90] U.S. DEP'T OF HEALTH & HUM SERVS., O.C.R., *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* (Nov. 26, 2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

[91] *See* Privacy Rule, 45 C.F.R. § 164.314 (2013); *see also id.* § 164.504(e)(2).

Similarly, the Genetic Information Nondiscrimination Act employs the secrecy paradigm in places[92] to protect genetic information by requiring entities subject to the act to keep such information as a "confidential medical record," and to withhold disclosure of it, unless a specific exception permits disclosure.[93] These demands place the full burden of privacy on the information's keeper.

The Video Privacy Protection Act ("VPPA")[94] also adopts the secrecy paradigm by prohibiting video tape service providers[95] from "knowingly disclos[ing] . . . personally identifiable information concerning any consumer."[96] Two circuit courts of appeals have ruled that the VPPA does not authorize a suit against a person who receives—as opposed to a service provider who discloses—personally identifiable information about a consumer.[97] Rather, it is the video tape service provider who must keep mum about the information once the information is received by someone else.

The secrecy paradigm's Achilles' heel is that in the age of digital technology and increasing surveillance, keeping information secret is formidably difficult, and one dribble of a digital crumb can bring a slew of consequences, including the loss of the right to harness the laws based on the secrecy paradigm to keep the information from being used by others. Technology has made it much easier to grab and keep data that was once functionally invisible.[98] Companies have greedily sucked up

---

[92] The GINA also employs the tactful inattention paradigm. *See infra* text accompanying notes 135–38.

[93] 42 U.S.C. § 2000ff-5 (2012) (confidentiality of genetic information); 29 C.F.R. § 1635.9(a)(1), (b) (2008).

[94] 18 U.S.C.A. § 2710 (West 2014).

[95] *Id.* § 2710(a)(4).

[96] *Id.* § 2710(b). Certain exceptions are available, including for disclosures "incident to the ordinary course of business." *Id.* § 2710(b)(2)(E).

[97] In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 281 (3d Cir. 2016); Daniel v. Cantrell, 375 F.3d 377, 382–84 (6th Cir. 2004).

[98] In *The Right to Privacy*, Samuel Warren and Louis Brandeis referred indirectly to the effect of technology in explaining why the tort of breach of confidentiality was inadequate to protect privacy:

> The narrower doctrine [of breach of contract] may have satisfied the demands of society at a time when the abuse to be guarded against could rarely have arisen without violating a contract or special confidence; but now that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation.

Warren & Brandeis, *supra* note 17, at 210–11.

information about consumers through their transactions, and then when they fail to sufficiently to protect the data they have amassed, it becomes a rich target for hackers.[99] Accordingly, Professors Woodrow and Hartzog describe the secrecy paradigm as "unworkable online" in part because "it simply does not reflect societal or individual notions of privacy."[100]

We could simply require people to avoid technology should they want to continue to keep private information now made accessible through technology. For instance, under old, snail-mail technology, the contents of a sealed letter are kept cloaked from prying eyes. However, email technology, which has replaced snail mail for many uses, reveals to those with access everything sent using the system. So, that argument goes, keep your information private by not using modern technology. However, letting technology vitiate long-standing privacy principles penalizes people who enjoy the benefits of technological advancement and who use them to fully participate in society.[101]

One scholar, Benjamin Zhu, has criticized "[t]he secrecy paradigm's focus on the private-public dichotomy [as] hinder[ing] the application of the intrusion tort to the data collection stage of

---

[99] *See, e.g.*, *Chronology of Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/data-breach (last visited Sept. 16, 2018) (identifying and describing data breaches from 2005 to the present); Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907, 908 (2013).

[100] Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CAL. L. REV. 1, 16–17 (2013). The authors describe a concept of obscurity founded in part by the court's reasoning in *Pietrylo v. Hillstone Restuarant Group*, in which a restaurant employee had created a closed group on a social network site that permitted visitors only with an invitation and a password. No. 06–5754 (FSH), 2008 WL 6085437, at *1 (D.N.J. July 25, 2008). One of the users showed the site to a restaurant manager, which led to other managers accessing it. *Id.* The site's creators sued the managers' employer, alleging, among other claims, invasion of privacy. *Id.* at *2. In denying the defendant's motion for summary judgment on that claim, the court stated, "Plaintiffs created an invitation-only internet discussion space [in which] they had an expectation that only invited users would be able to read the discussion." *Id.* at *6. Professors Hartzog and Stutzman argue that "[b]y giving such weight to password protections, *Pietrylo* laid the foundation for a concrete concept of obscurity." Hartzog & Stutzman, *supra* note 100, at 27. Other cases focusing on password protection, say the authors, "suggest[] that courts are willing to depart from the rule that individuals have no expectation of privacy in information posted online." *Id.* at 28.

[101] *See* Andrew J. DeFilippis, Note, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1091–92 (2006) (noting the effects on privacy of our transformation to a digital society, and stating that "to ask a person to refrain from using e-mail for fear of its recordability is to ask him to live a premodern life.").

dataveillance."[102] Professor Patricia Sánchez Abril similarly criticized the secrecy paradigm's application to modern data practices, noting that "[i]n cyberspace, the complete secrecy requirement of privacy torts is difficult, if not impossible, to satisfy. Total secrecy is difficult offline; this difficulty is magnified online."[103]

A different approach to this accessibility advance is to adapt the secrecy paradigm to the new technology by pretending that the access has not arisen. For instance, although the attorney-client privilege is generally waived when an attorney communicates otherwise confidential information to a client in front of a third party,[104] several courts have ruled that using email to communicate confidential information will not void the privilege–even though the technology has the capability of revealing the information to any number of potential watchers along the way.[105] This is something of a "secrecy fiction," but one

---

[102] Benjamin Zhu, *A Traditional Tort for a Modern Threat: Applying Intrusion upon Seclusion to Dataveillance Observations*, 89 N.Y.U. L. REV. 2381, 2397 (2014). Professor Zhu cites two Illinois cases that illustrate this shortcoming of the secrecy paradigm. In *Busse v. Motorola, Inc.*, a class of mobile phone customers alleged that their service providers had transferred their customer data to a private research firm, including names, addresses, and dates of birth, for its own study; the court held that no intrusion had occurred because the information was not private. 813 N.E.2d 1013, 1017 (Ill. App. Ct. 2004). Similarly, in *Dwyer v. American Express Co.*, charge card holders challenged the defendants' practice of renting to third parties lists compiling their spending information; the court held that no unauthorized intrusion occurred, because "[b]y using the American Express card, a cardholder is voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences." 652 N.E.2d 1351, 1354 (Ill. App. Ct. 1995).

[103] Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J.L. & TECH. 1, 25 (2007). As an example, Professor Abril cites *Wilson v. Harvey*, 842 N.E.2d 83 (Ohio Ct. App. 2005). In that case, a college student sued three fellow students who had put up flyers around campus with the plaintiff's name, email, and phone number that depicted him as a homosexual. *Id.* at 86. The appellate court affirmed a directed verdict on the student's public disclosure of private facts claim, reasoning that none of the published information was private because "it was published in various forms obtainable by university students and faculty." *Id.* at 91.

[104] *See* Lluberes v. Uncommon Prods., LLC, 663 F.3d 6, 24 (1st Cir. 2011); *see generally*, 2 Paul R. Rice, ATTORNEY–CLIENT PRIVILEGE IN THE U.S. § 9:79 (2017).

[105] *See, e.g.*, In re Asia Glob. Crossing, Ltd., 322 B.R. 247, 251 (Bankr. S.D.N.Y. 2005) (concluding that communicating with one's attorney via email does not, without more, waive the protection of the attorney-client privilege); City of Reno v. Reno Police Protective Ass'n, 59 P.3d 1212, 1218 (Nev. 2002). A third party's presence will generally not nullify the privilege where the third party is a necessary participant to the conversation. *See, e.g.*, PSE Consulting, Inc. v. Frank Mercede &

that may be justified by the policies underlying the confidentiality privilege.

II. DEVELOPMENT OF TACTFUL INATTENTION

We exercise tactful inattention in our social interactions. As Jeffrey Rosen has pointed out, "it[i]s considered rude to stare at strangers whom you encounter in public."[106] For instance, to use a real-territory (rather than a cyber-territory) example, an American bathroom stall affords privacy but not through ironclad barriers to prying eyes—they usually have gaps at the top and bottom edges and between the door and its frame.[107] Nonetheless, we justifiably expect that notwithstanding these points of access, others will avert their eyes from our vulnerabilities when we are within that space. One scholar of privacy and design invokes Goffman's "civil inattention" to describe it as a "device of scrupulously observed avoidance behavior . . . [that] demands that we avoid observing other people's behavior . . . ."[108]

Tactful inattention may be a concept recognized more readily by some other cultures. For instance, in Germany it is possible that one may appear fully nude in a public park, yet maintain a culturally-accepted belief that one is entitled to not be stared at, that is, to be entitled to have others avert their eyes from the display of nudity.[109] One author characterizes this practice as "respectful 'civil inattention.' "[110]

Sons, Inc., 838 A.2d 135, 167 n.28 (Conn. 2004); People v. Osorio, 75 N.Y.2d 80, 84, 549 N.E.2d 1183, 550 N.Y.S.2d 612 (1989).

[106] JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 16 (2000) (citing GOFFMAN, *supra* note 5, at 84–85, 116).

[107] However, one author has emphasized the difference in architectural design of American public bathrooms, and their fostering of policing functions, compared with those in Europe, where complete "floor-to-ceiling enclosures" are more common. ALEXANDER KIRA, THE BATHROOM 204–05 (Viking Press 1976).

[108] *Id.* at 204. We do this by "try[ing] to ignore the presence of other problems while at the same time acknowledging them by being careful not to intrude on their privacy." *Id.* He describes the example of diners in Soviet restaurants, "which have the disconcerting habit, for us, of filling every empty seat with unrelated diners." *Id*. Accordingly, an unrelated pair of diners seated at a table for four "can preserve their privacy only . . . by mutually practicing civil inattention or avoidance behavior . . . " *Id.* at 204. He points out that "[c]ivil inattention" as a term describes our "instinctive[] realiz[ation] that the delicate behavioral devices that guarantee our privacy and that of our neighbors is a mutually dependent exercise." *Id*.

[109] *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1201 (2004) ("As any German there will tell you, it is a matter of ordinary politeness that nude people have a right not to be stared at.

A. Traditional Examples of Tactful Inattention in Law

The expectation of tactful inattention arises not only in social settings; it also exists in legal expectations. While the secrecy paradigm is common,[111] the concept of mandating tactful inattention already appears in some laws. Sometimes the law directs itself to tactful inattention from the start, prohibiting an initial capture of others' information, and sometimes it directs itself to post-capture behavior, prohibiting the use of the information.

1. Tactful Inattention by Prohibiting the Capture of Available Information

"Peeping Tom" statutes represent an early attempt to encourage the averting of eyes.[112] They do not restrict criminal liability to those situations where the target has taken all possible steps to limit access to view, but rather put some onus on the peeper to confine his gaze.[113] For instance, Louisiana defines a "Peeping Tom" as "one who peeps through windows or doors . . . situated on or about the premises of another . . . for the purpose of spying upon or invading the privacy of persons spied upon."[114] Curiously, Peeping Tom statutes tend not to specifically define the verb "peep." The Oxford English Dictionary defines it as "[t]o look through a narrow aperture . . . to look quickly or furtively from a vantage point; to steal a glance."[115] The fact that

---

Taking off all your clothes, even in a public park, does not constitute a surrender of your privacy.").

[110] CARLIN A. BARTON, ROMAN HONOR: THE FIRE IN THE BONES 204 n.18 (2001).

[111] *See supra* text accompanying notes 8–11.

[112] *See, e.g.*, H. Morley Swingle & Kevin M. Zoellner, *Criminalizing Invasion of Privacy: Taking a Big Stick to Peeping Toms*, 52 J. MO. B. 345, 345 (1996). The term "Peeping Tom" derives from the legend of Lady Godiva, whose husband, the Earl of Mercia, promised to repeal ruinous taxes that he'd levied on the citizens of Coventry if she dared to ride through the town's market on horseback nude. *See* RONALD AQUILLA CLARKE & PATRICK A.E. DAY, LADY GODIVA: IMAGES OF A LEGEND IN ART & SOCIETY 8 (1982). The legend was made famous by the poem of Alfred Lord Tennyson, where he described "one low churl . . . /Peep'd—but his eyes before they had their will,/Were shrivell'd into darkness in his head,/And dropt before him." Alfred, Lord Tennyson, *Godiva* (1842).

[113] *See*, *e.g.*, GA. CODE ANN. § 16–11–61 (2016); LA. STAT. ANN. § 14:284 (2016); OKLA. STAT. ANN. tit. 21, § 1171 (2008).

[114] LA. STAT. ANN. § 14:284.

[115] *Peep*, THE OXFORD ENGLISH DICTIONARY (2d ed. 1989).

visual access can be won from outside the premises does not mean that the regarder is entitled to the view. Rather, the regarder must shift the gaze elsewhere.[116]

Anti-recording laws, such as the Electronic Communication Privacy Act's Wiretap Act, can also present as tactful inattention laws; they prohibit a person from interacting in a particular way with the information—the intercepting of it.[117] The listener remains free to use the content of the information in indirect discourse, along the lines of "he said '____.' " However, the listener may not target the speech as the object of his or her recording device.[118]

2. Prohibiting the Use of Captured Information

The tactful inattention paradigm can also present as the prohibition not of the capture or possession of sensitive information, but the use of it for a particular purpose. For example, the crime of blackmail criminalizes the blackmailer's use of embarrassing information to serve a particular purpose—to manipulate the target. In this context, the tactful inattention paradigm combats directly the abuse of access to and possession of sensitive information, and the imbalance in power that arises out of blackmail.[119] Prohibiting blackmail, Solove says, "prevents

---

[116] *See, e.g.*, GA. CODE ANN. § 16–11–61 ("Peeping Tom"); LA. REV. STAT. ANN. § 14:284 ("Peeping Tom; penalties"); N.C. GEN. STAT. ANN. § 14–202 (2017) ("peep[ing] secretly into any room occupied by another person"); S.C. CODE ANN. § 16–17–470 (2018) ("[e]avesdropping, peeping, voyeurism"); VA. CODE ANN. § 18.2–130 (2018) ("[p]eeping or spying into a dwelling or enclosure").

[117] Wiretap Act, 18 U.S.C. § 2511(1)(a) (2012). Not only does the Wiretap Act prohibit the intercepting of specified communications, it forbids one from using data that one knows has been recorded in violation of the Act. Also, note that the statute forbids the use of data you know has been illegally recorded. *Id.* § 2511(c). This provision has faced constitutional challenges. *Compare* Bartnicki v. Vopper, 532 U.S. 514 (2001) (individual who had played no role in illegally intercepting a communication could not be liable for broadcasting it where it concerned matters of public concern) *with* Boehner v. McDermott, 484 F.3d 573 (D.C. Cir. 2007) (First Amendment did not preclude enforcement of provision against a Congressman who obtained tape of a telephone conversation where he was a member of the Congressional Ethics Committee, which subjected him to independent nondisclosure rules).

[118] *See generally* 18 U.S.C. § 2511.

[119] *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 543 (2006) [hereinafter Solove, *A Taxonomy of Privacy*] ("With blackmail, the harm is not in the actual disclosure of the information, but the control exercised by the one who makes the threat over the data subject.").

people from taking advantage of us with our personal information."[120] It also requires the blackmailer to "inattend" the sensitive information—though perhaps not exactly "tactfully."[121]

In terms of regulating personal identity, false impersonation laws, which are precursors to modern state identity theft prohibitions,[122] also exemplify a sort of tactful inattention model. That is, the statutes generally do not criminalize the acquisition of the data,[123] or its disclosure, but its specific use for identified purposes, such as to obtain something of value.[124]

Tactful inattention is also a feature of evidence law, where a jury might be instructed that a specific item of information may be considered for one purpose, but may not be considered for another.[125]

In the civil context, a typical trade secrets law may forbid one from using a trade secret known to a person if that person knows, or should know, that the trade secret was acquired improperly.[126] As Professor Sharon Sandeen writes, the doctrine of "relative secrecy" allows for information to continue to benefit from the trade secret doctrine even when known by several individuals or entities.[127] The fact that someone outside the

---

[120] *Id.* at 544.

[121] *See supra* Introduction.

[122] *See, e.g.*, 720 ILL. COMP. STAT. ANN. 5/16–30 (West 2018) (defining "identity theft" and "aggravated identity theft"); N.Y. PENAL LAW § 190.80 (MCKINNEY 2008) (defining "identity theft in the first degree"). *But see* 720 ILL. COMP. STAT. ANN. 5/16–31(a) (defining the crime of "transmission of personal identifying information," which applies when "information is photographed or otherwise captured, recorded, distributed, disseminated, or transmitted" without the consent of the person about whom the information pertains). This would exemplify the "secrecy" paradigm rather than the "tactful inattention" paradigm.

[123] *See, e.g.*, CAL. PENAL CODE § 529 (West 2018) (originally enacted in 1872); FLA. STAT. ANN. § 817.02 (West 2018) (originally enacted in 1868); MASS. GEN. LAWS CH. 266, § 71 (West 2018).

[124] *See, e.g.*, CAL. PENAL CODE § 529; FLA. STAT. ANN. § 817.02; MASS. GEN. LAWS ANN. ch. 266, § 71.

[125] FED. R. EVID. 105 provides that "[i]f the court admits evidence that is admissible against a party or for a purpose—but not against another party or for another purpose—the court, on timely request, must restrict the evidence to its proper scope and instruct the jury accordingly." Some scholars have expressed skepticism about the efficacy of curative or limiting instructions. *See, e.g.*, Dan Simon, *More Problems with Criminal Trials: The Limited Effectiveness of Legal Mechanisms*, 75 L. & CONTEMP. PROBS., 167, 177–180 (2012).

[126] *See, e.g.*, 765 ILL. COMP. STAT. ANN. 1065/2(b)(1) (West 2018) (defining misappropriation).

[127] Sharon K. Sandeen, *Relative Privacy: What Privacy Advocates Can Learn from Trade Secret Law*, 2006 MICH. ST. L. REV. 667, 696 (2006). She describes the

"backstage area" now possesses the trade secret does not destroy the protection. Somewhat similarly, the Fourth Amendment's exclusionary rule prohibits the use of information acquired through an unconstitutional search, at least in some circumstances.[128]

The need for tactful inattention often occurs as a result of a secondary use of information, which in Professor Solove's taxonomy is "the use of data for purposes unrelated to the purposes for which the data was originally collected without the data subject's consent."[129] Professor Solove identifies the harm from secondary use as a "dignitary harm," arguing that "[s]econdary uses thwart people's expectations about how the data they give out will be used."[130] Furthermore, he notes that data that is "removed from the original context in which it was collected . . . can more readily be misunderstood."[131] The Fair Information Practices set out by the U.S. Department of Health, Education, and Welfare incorporate this limit of secondary use by providing that "[t]here must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent."[132] The federal Driver's Privacy Protection Act of 1994 implements this limitation on secondary use by making it "unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted [by the Act]."[133] This type of required tactful inattention has also been called "use regulation."[134]

---

law as "recogniz[ing] legal rights in the originator . . . depend[ing] upon the circumstances of disclosure." *Id.* at 697.

[128] *See* Weeks v. United States, 232 U.S. 383, 398 (1914).

[129] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 129–33 (2008).

[130] Solove, *A Taxonomy of Privacy*, *supra* note 119, at 521.

[131] *Id.*

[132] U.S. DEP'T OF HEALTH, EDUC., & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS 41 (1973).

[133] Driver's Privacy Act of 1994, 18 U.S.C. § 2722 (2012).

[134] Chris Jay Hoofnagle, *The Potemkinism of Privacy Pragmatism: Civil Liberties Are Too Important To Be Left to the Technologists*, SLATE (Sept. 2, 2014, 8:36 AM), http://www.slate.com/articles/technology/future_tense/2014/09/data_use_regulation_the_libertarian_push_behind_a_new_take_on_privacy.html.

C. Modern Adoptions of Tactful Inattention in Law

This part discusses four areas of modern legislation that incorporate the tactful inattention paradigm.

1. The Genetic Information Nondiscrimination Act

The Genetic Information Nondiscrimination Act (the "GINA") is an example of the tactful inattention and secrecy paradigms working together within a single law.[135] The GINA requires covered entities to keep genetic information confidential, subject to certain limited exceptions, a secrecy paradigm feature.[136] But it also acknowledges that sometimes such data may be revealed, and steps forward to limit the use of such information by prohibiting employers from discriminating against employees because of genetic information.[137] The legislators who passed the GINA seemed to recognize that some prohibited uses of genetic information may be rational, even otherwise beneficial to the user, but that nonetheless, other values—including privacy—outweigh that justification.[138]

2. The Fair Credit Reporting Act

The Fair Credit Reporting Act ("FCRA") also uses features of both the tactful inattention paradigm and the secrecy paradigm, showing that they are not entirely exclusive, but can complement each other. The FCRA prohibits consumer reporting agencies from reporting some adverse information that Congress designated as obsolete.[139] Thus, in general, an agency may not insert into consumer reports certain adverse items of information

---

[135] Genetic Information Nondiscrimination Act, 42 U.S.C. § 2000ff-11 (2012).

[136] *Id.* § 2000ff-5.

[137] *Id.* § 2000ff-1(a) (prohibiting discrimination by employers); *Id.* § 2000ff-2(a) (prohibiting discrimination by employment agencies); *Id.* § 2000ff-3(a) (prohibiting discrimination by labor organizations); 29 C.F.R. § 1635.9(a) (2016) (requiring confidentiality, prohibiting disclosure).

[138] *See* 42 U.S.C. § 2000ff-1(a) (defining certain prohibited employment practices based on genetic information). Solove notes that there's a purpose in prohibiting the penalization of "people for things they cannot control." Solove, *A Taxonomy of Privacy*, *supra* note 119, at 533.

[139] Fair Credit Reporting Act, 15 U.S.C. § 1681c(a) (2012).

it has acquired that are more than seven years old.[140] However, the FCRA reinstates obsolete information's eligibility for certain large-scale transactions and employment.[141]

The FCRA's obsolescence provisions illustrate the tactful inattention paradigm by prohibiting consumer reporting agencies from publicizing information that they may have acquired about a consumer.[142] The provisions also have features of the secrecy paradigm in that the agencies must keep such information secret while simultaneously averting their eyes from it.

3. Pre-Existing Employee "Lifestyle" Laws

Many states prevent employers from freely using information about an employee's personal activities that they might come across (or scour for) against such employees; sometimes employers are forbidden from even keeping a record of them.

For example, the state of Michigan forbids employers from "gather[ing] or keep[ing] a record of an employee's associations, political activities, publications, or communication of nonemployment activities."[143] However, the statute does permit employers to monitor such activities that occur on the employers' premises or during working hours and that "interfere with the performance of the employee's duties or duties of other employees."[144] Similarly, New York protects a broad category of employee "recreational activities," from employer discrimination, including "sports, games, hobbies, exercise, reading and the

---

[140] *Id.* § 1681c(a)(5). Criminal convictions are exempt from the prohibition. *Id.* § 1681c(a)(5). And bankruptcies don't become stale until after ten years. *Id.* The Fair Credit Reporting Act provides specific designations for the time from which the identified period runs for bankruptcies, civil suits, civil judgments, records of arrest, paid tax liens, and accounts placed for collection that help determine when the seven-year period starts. *Id.* § 1681c(a)(1)–(4), (c). These obsolescence provisions have withstood a First Amendment challenge. King v. Gen. Info. Servs., 903 F. Supp. 2d 303, 306, 313 (E.D. Pa. 2012). The obsolescence provisions pertain only to negative information; the Act does not restrict the reporting of old positive information. *See generally* 15 U.S.C. § 1681c.

[141] 15 U.S.C. § 1681c(b).

[142] *Id.* § 1681c(a).

[143] MICH. COMP. LAWS ANN. § 423.508(1) (West 2018).

[144] *Id.*

viewing of television, movies and similar material."[145] Other states with similar laws include Montana,[146] North Dakota,[147] and Colorado.[148]

These laws express the tactful inattention paradigm by acknowledging implicitly that personal information not sufficiently impinging on that employee's work should not play a role in the employers' assessments. Employers must avert their eyes from such information, regardless of the efforts or lack thereof the employee has made to hide the information. In this way, these lifestyle laws are a model for similar laws.

4. Employer Use of Credit Reports and Criminal Records

Recently, states have begun to regulate the use by employers of their applicants' credit reports and even their criminal records. This background information is often easily available from consumer reporting agencies, and certainly the federal FCRA permits such investigation by employers.[149] However, some states have recognized that even though certain information may be accessible, it nonetheless should not always play a role in

---

[145] N.Y. LAB. LAW § 201-d(1)(b) (MCKINNEY 2018). New York permits employers to allow themselves to be influenced by such activities if they occur during working hours or on the employer's premises, and also where the activities "create[] a material conflict of interest related to the employer's . . . business interest." *Id.* § 201-d(3)(a). Other exceptions also exist. *Id.* § 201-d(3)(b)-(e).

[146] MONT. CODE ANN. § 39-2-903(5) (West 2017) (generally prohibiting employers from firing employees without "good cause," and specifically identifying "[t]he legal use of a lawful product by an individual off the employer's premises during nonworking hours" as not being a good cause). As is typical of such laws, an employer may act upon that information in certain narrow circumstances where the employer's interests are affected. *Id.* § 39-2-313.

[147] N.D. CENT. CODE ANN. § 14-02.4-03 (West 2017) (designating as a "discriminatory practice" the making of employment decisions because of an employee's "participation in lawful activity off the employer's premises during nonworking hours" so long as the activity is "not in direct conflict with the essential business-related interests of the employer").

[148] COLO. REV. STAT. ANN. § 24-34-402.5(1) (West 2018) (declaring it an "unfair employment practice" for an employer to terminate employment because of "lawful activity" that occurs off the employer's premises and during nonworking hours unless the restriction either "[r]elates to a bona fide occupational requirement or is reasonably and rationally related to the employment activities and responsibilities of a particular employee or a particular group of employees" or "[i]s necessary to avoid a conflict of interest" or the appearance of such with the employer's responsibilities).

[149] *See* Fair Credit Reporting Act, 15 U.S.C. § 1681b(a)(3)(B) (2012) (permitting consumer reporting agencies to furnish consumer reports to those who "intend[] to use the information for employment purposes"). The act imposes conditions on the agencies for furnishing such reports, though. *Id.* § 1681b(b).

employment decisions.[150] Below, employer use of credit reports is discussed first, followed by employer use of criminal record information.

a. Employer Use of Credit Reports

The tactful inattention paradigm appears in recent state laws that limit employers from considering applicants' credit reports in making hiring decisions. California, Colorado, Connecticut, Delaware, Hawaii, Illinois, Maryland, Nevada, Oregon, Vermont, and Washington have all passed credit history cloaking measures.[151] In addition, Washington, D.C. incorporated such a limitation into its human rights law.[152]

Credit history cloaking laws have some common features. In general, the statutes apply to similar types of information—a report that contains information about the applicant's credit history.[153] The strictest laws prohibit employers from even *obtaining* a report, implementing tactful inattention by requiring the averting of eyes up front.[154] Typically, they forbid employers from acting on the contents of a credit report—that is, discriminating on the basis of credit information.[155] Connecticut

---

[150] CAL. CIV. CODE § 1785.20.5 (West 2018); CAL. LAB. CODE § 1024.5 (West 2018); COLO. REV. STAT. ANN. § 8-2-126 (West 2018); COLO. CODE REGS. §§ 1103-4:1, 1103-4:12 (2018); CONN. GEN. STAT. ANN. § 31-51tt (West 2018); DEL. CODE ANN. tit. 19, § 711(g) (West 2018); HAW. REV. STAT. ANN. § 378-2(a)(8) (West 2017); 820 ILL. COMP. STAT. ANN. 70/5, 70/30 (West 2018); MD. CODE ANN. LAB. & EMPL. § 3-711 (West 2018); NEV. REV. STAT. ANN. § 613.570 (West 2017); OR. REV. STAT. ANN. § 659A.320 (West 2018); VT. STAT. ANN. tit. 21, § 495i (West 2018); WASH. REV. CODE ANN. § 19.182.020(2)(c) (West 2018).

[151] CAL. CIV. CODE § 1785.20.5; CAL. LAB. CODE § 1024.5; COLO. REV. STAT. ANN. § 8-2-126; COLO. CODE REGS. §§ 1103-4:1, 1103-4:12; CONN. GEN. STAT. ANN. § 31-51tt; DEL. CODE ANN. tit. 19, § 711(g); HAW. REV. STAT. ANN. § 378-2(a)(8); 820 ILL. COMP. STAT. ANN. 70/5, 70/30; MD. CODE ANN. LAB. & EMPL. § 3-711; NEV. REV. STAT. ANN. § 613.570; OR. REV. STAT. ANN. § 659A.320; VT. STAT. ANN. tit. 21, § 495i; WASH. REV. CODE ANN. § 19.182.020(2)(c).

[152] D.C. Code Ann. § 2-14-2.11(a)(4)(D) (West 2018) (text applicable upon the date of inclusion of its fiscal effect in an approved budget and financial plan).

[153] *See, e.g.*, CAL. CIV. CODE § 1785.20.5(a); CAL. LAB. CODE § 1024.5(a); CONN. GEN. STAT. ANN. § 31-51tt(b); 820 ILL. COMP. STAT. ANN. 70/5; MD. CODE ANN. LAB. & EMPL. § 3-711(b); VT. STAT. ANN. § 495i(a)(2), (3); WASH. REV. CODE ANN. § 19.182.010(4).

[154] D.C. CODE ANN. § 2-14-2.11(a)(4)(D) (forbidding employers from, among other acts, "us[ing] . . . an employee's credit information"); OR. REV. STAT. ANN. § 659A.320(1); VT. STAT. ANN. § 495i(b)(2) (forbidding employers from "[i]nquir[ing] about an applicant or employee's credit report or credit history"); WASH. REV. CODE ANN. § 19.182.020(c).

[155] CAL. LAB. CODE § 1024.5(a); DEL. CODE ANN. tit. 19, § 711(g)(1); HAW. REV. STAT. ANN. § 378-2(a)(8); 820 ILL. COMP. STAT. ANN. 70/10(a); MD. CODE ANN. LAB. &

has the weakest prohibition. It merely bars employers from requiring an employee or applicant to consent to a request for a credit report but does not prohibit an employer from making the request, even though applicants might not feel free to deny it.[156] It can perhaps be characterized as a suggestion that the employer avert its eyes, putting more of a burden on the holder of the key to the information—the employee or applicant who must consent—to withhold the information's accessibility by denying consent.[157]

The tactful inattention paradigm is evident in different ways in these laws. Essentially, the laws tell employers that even though information about an applicant or employee is available, nonetheless they must avert their eyes from it or, if they see it, must avoid using it in making their human resources decisions.

Of course, these prohibitions have exceptions, some of which threaten to swamp the rule.[158] Still, these laws acknowledge

---

EMP. § 3-711(b), (c) (use for a non-prohibited purpose); OR. REV. STAT. ANN. § 659A.320(1); 21 VT. STAT. ANN. tit. 21, § 495i(b). Nevada comes close to prohibiting the acquisition of a report, forbidding employers from inquiring concerning a consumer credit report. NEV. REV. STAT. § 613(7)(3).

[156] CONN. GEN. STAT. ANN. § 31-51tt(b).

[157] *Id.*

[158] For instance, most of the laws exempt some types of management positions. CAL LAB. CODE § 1024.5(a)(1); CONN. GEN. STAT. ANN. § 31-51tt(a)(4)(A) (managerial positions), (C) (fiduciary positions); MD. CODE ANN. LAB & EMPL. § 3-711(c)(2)(i); NEV. REV. STAT. § 613.580(3)(c) (West 2017); 820 ILL. COMP. STAT. ANN. 70/10(b)(4) (exempting those positions for which "a satisfactory credit history is an established bona fide occupational requirement," a feature that requires the presence of at least one of seven designated circumstances, one of which is that the position is managerial); VT. STAT. ANN. § 495i(c)(1)(E) (positions requiring "a financial fiduciary responsibility to the employer or a client of the employer"); *see also* HAW. REV. STAT. § 378-2.7(a)(1) (credit history is related to a bona fide occupational requirement and the employee has received a conditional offer of employment), *id.* § 378-2.7(a)(3) (the position is managerial or supervisory). Other positions commonly exempted include those with financial institutions or that involve monetary transactions. *See, e.g.*, CAL. LAB. CODE § 1024.5(b) (institutions covered by the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809); *id.* § 1024.5(a)(5)(A)-(C) (access to bank or credit card information along with an individual's date of birth and Social Security Number, excluding routine credit card transactions); *id.* § 1024.5(a)(8) (positions involving regular access to cash totaling $10,000 or more); CONN. GEN. STAT. ANN. § 31-51tt(b) (financial institutions); D.C. CODE ANN. § 2-1402.11(d)(6) (West 2018) (duties of the position "involves access to personal financial information"); HAW. REV. STAT. ANN. § 378-2.7(a)(4); 820 ILL. COMP. STAT. ANN. 70/5 (excluding from the definition of "employer"), 70/10(b)(2), (3) (duties of the position include access to cash or assets worth $2500 or more, or signatory power over assets of $100 or more); MD. CODE ANN. LAB. & EMPL. § 3-711(c)(2)(iii) (involves a fiduciary responsibility, including collecting payments, and for those who are provided an expense account or corporate debit or credit card); NEV. REV.

that, with our information, an attitude of "finders-keepers" toward sensitive information may not strike the sort of balance that will allow individuals to fully flourish.[159]

b. Employers' Use of Criminal Record Information

The tactful inattention paradigm also appears in recent state legislation restricting private employers from inquiring into or considering the criminal record of job applicants. The practice is common: a 2012 survey by the Society for Human Resource Management reveals that 69% of employers investigate the criminal background of every applicant.[160] Such public record information has become much more widely available. At one time, a comprehensive criminal background check would have required a county-by-county visit to clerk counters across the country, but now, many records are available online so that an individual's record can be checked from a desk, or even a smartphone.[161]

While it seems intuitively obvious why employers would want to know of any criminal taint on an applicant's past, employee advocates worry that a criminal record—even a single record of arrest—can unjustifiably isolate a candidate from positions that do not necessarily require an unblemished background.[162] The numbers of those affected are not small: 8.6% of American adults have a felony conviction, and approximately 65 million Americans have some kind of criminal record.[163] Accordingly, advocacy groups such as the National Employment

STAT. § 613.570 (3)(a); OR. REV. STAT. ANN. § 659A.320(2)(a) (federally insured banks or credit unions); VT. STAT. ANN. tit. 21, § 495i(c)(1)(B), (C), (G); (access to confidential financial information and the employer's payroll, respectively).

[159] *See supra* text accompanying notes 153–57 .

[160] Society for Human Resource Management, *SHRM Survey Findings: Background Checking—The Use of Criminal Background Checks in Hiring Decisions*, SLIDESHARE (August 15, 2012), http://www.slideshare.net/shrm/2012-backgroundcheck-criminalfinal (turn to page three on the slideshow).

[161] FTC, *FTC Warns Marketers That Mobile Apps May Violate Fair Credit Reporting Act* (Feb. 7, 2012), http://www.ftc.gov/opa/2012/02/mobileapps.shtm.

[162] Am. Civil Liberties Union et al, *State Reforms Reducing Consequences for People with Criminal Records: 2011-2012 Legislative Round-Up*, NAT'L EMP'T LAW PROJECT 1 (Sept. 2012), http://www.nelp.org/content/uploads/2015/03/StateCollateralConsequencesLegislativeRoundupSept2012.pdf.pdf.

[163] *Id.*

Law Project have urged states to reform their employment laws to reduce the impact of a criminal background on an applicant's candidacy.[164]

Responding to such concerns, some state credit reporting statutes restrict agencies from putting certain criminal record information into consumer reports.[165] These restrictions vary widely. New York, with one of the more robust provisions, flatly prohibits agencies from reporting criminal arrest information for past charges unless the individual was convicted of the offense.[166] Furthermore, the state prohibits the reporting of criminal convictions more than seven years old unless an exception applies.[167] Similarly, California prohibits not only the reporting of criminal record information that is more than seven years old, but also the reporting of any pardoned convictions or other arrests, indictments, or similar information where no conviction followed.[168] Nonetheless, exclusions of criminal record information are often themselves subject to an exclusion, returning such information to an employee's credit report.[169]

However, even where criminal record information is available on an applicant's background checks or similar credit report, some states limit what employers may ask about or consider in terms of an applicant's criminal record.[170] This is a tactful inattention approach because the information may be available to an employer, but the employer must take efforts to avoid looking at it or considering it. States with restrictions on private employers include California,[171] Hawaii,[172] Illinois,[173]

---

[164] *Id.*

[165] *See infra* text accompanying notes 166–69.

[166] N.Y. GEN. BUS. LAW. § 380-j(a)(1) (McKinney 2018). The statute does permit a consumer reporting agency to disclose the detention of the consumer by a retail mercantile establishment so long as he or she has executed an uncoerced admission of wrongdoing, and received a prescribed notice from the establishment. *Id.* § 380-j(b).

[167] *Id.* § 380-j(f)(1)(v).

[168] CAL. CIV. CODE § 1785.13(a)(6) (West 2018).

[169] *See supra* text accompanying notes 165–68.

[170] *See infra* notes 171–75.

[171] CAL. LAB. CODE § 432.7 (West 2018) (forbidding employers from asking an applicant to disclose information regarding arrests or detentions that did not result in conviction, and prohibiting employers from seeking such information, but designating exceptions).

[172] HAW. REV. STAT. ANN. § 378-2.5 (West 2017).

[173] 820 ILL. COMP. STAT. ANN. §§ 75/10, 75/15 (West 2018) (applying to private employers with fifteen or more employees, and prohibiting them from inquiring into or considering an applicant's criminal history until the applicant has been deemed

Massachusetts,[174] Minnesota,[175] New Jersey,[176] and Rhode Island.[177] Hawaii's statute, for example, provides that an employer may "inquire about and consider an individual's criminal conviction record" only after the prospective employee has received a conditional offer of employment, and only where "the conviction record bears a rational relationship to the duties and responsibilities of the position."[178] Some states have enacted provisions restricting criminal history inquiries for positions in public agencies, as opposed to those with private employers.[179]

Here, too, the tactful inattention paradigm appears. Criminal records are, after all, public records, available in many states online, and even on smartphone apps that are available to

---

qualified and either has been notified of an interview or has received a conditional offer of employment).

[174] MASS. GEN. LAWS ANN. ch. 151B, § 4(9 ½) (West 2018) (prohibiting employers from requesting criminal record information on initial application forms, though with certain exceptions).

[175] MINN. ST. ANN. § 364.021 (West 2018) (prohibiting private employers from inquiring into or considering an applicant's criminal record history, also with certain specific exceptions).

[176] N.J. STAT. ANN. §§ 34:6B-11–34:6B-14 (West 2018) (prohibiting employers with fifteen or more employees, and prohibiting employers from asking about an applicant's criminal record "during the initial employment application process").

[177] R.I. GEN. LAWS ANN. § 28-5-7 (West 2017).

[178] HAW. REV. STAT. ANN. § 378-2.5 (West 2017). As an example of a weaker protection, Rhode Island merely prohibits employers from including questions as to an applicant's criminal record on employment applications, while permitting employers to ask applicants about criminal convictions (though apparently not about arrests or charges not resulting in convictions) at the first interview or later. R.I. GEN. LAWS ANN. § 28-5-7.

[179] *See, e.g.*, COLO. REV. STAT. ANN. § 24-5-101 (West 2018) (limiting the consideration of a criminal record in applicants for public employment); CONN. GEN STAT. ANN. § 46a-80 (West 2018) (providing that an applicant will not be disqualified from employment by the state "solely because of a prior conviction of a crime," with exceptions); DEL. CODE ANN. tit. 19, § 711(g)(1) (West 2018) (prohibiting public employers from inquiring into or considering the criminal record or history, along with credit history or credit score, during the initial application process, with exceptions); MD. CODE ANN. STATE PERS. & PENS. § 2-203 (West 2018) (effective July 1, 2018, and prohibiting public employers (with exceptions) from inquiring into an applicant's criminal history until after the applicant has been provided an opportunity to interview); NEB. REV. STAT. ANN. § 48-202 (West 2018) (prohibiting public employers from asking for an applicant's criminal history "until the public employer has determined the applicant meets the minimum employment qualifications," providing exceptions); N.M. STAT. ANN. § 28-2-3 (West 2018) (prohibiting public employers from considering misdemeanor convictions not involving moral turpitude and arrest records not followed by conviction, and further prohibiting such employers from inquiring about criminal convictions on initial applications and from considering them before the applicant has been selected as a finalist).

all.[180] Similarly, the FCRA permits employers, among others, to access employees' credit reports and expressly acknowledges that employment purposes are justifiable reasons to access a credit report.[181] Such state limits on access express the belief that simply because data exists and one has the means to grab it, does not mean one should grab it—no peeping permitted.

Even when a statute eventually permits a peek at a criminal record, such as Hawaii's provision,[182] the statute requires tactful inattention until the employer has a concrete reason to "attend" to this aspect of an employee or candidate's past.

III. EMERGING AREAS OF TACTFUL INATTENTION IN LAW

The tactful inattention paradigm offers a possible path for protecting privacy in the big data age. Instead of requiring individuals to make Herculean efforts to avoid dribbling data, we instead can require observers to make modest efforts to avoid peeping at or using, it.[183] We can, in effect, require the use of virtual blinkers, and, as discussed above, have done so both traditionally and recently.

A. Employers' Examination of Social Media

One area of conflict that could benefit from a tactful inattention paradigm is the use by employers of the information employees and applicants put on social media such as Facebook and Twitter. Requiring employers to limit their gaze on and their use of such information would allow individuals to fully benefit from these new technologies and the relationships that they underlie and promote, without having to hide the information from those who might use it to harm them.[184]

---

[180] *See, e.g.*, In re Filiquarian Publ'g, LLC, No. C-4401 (Apr. 30, 2013) (decision and order), http://www.ftc.gov/sites/default/files/documents/cases/2013/05/130501filquariando.pdf.

[181] Fair Credit Reporting Act, 15 U.S.C. § 1681b(a)(3)(B) (2012).

[182] HAW. REV. STAT. ANN. § 378-2.5(a)-(b) (West 2018).

[183] Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIAMI L. REV. 559, 599–600 (2015).

[184] Josh Eidelson, *Can You Be Fired for What You Post on Facebook*?, SLATE (July 3, 2012, 4:40 PM), http://slate.com/articles/news_and_politics/jurisprudence/2012/07/getting_fired_for_what_you_post_on_facebook.html. Labor law has already intervened to regulate the use by employers of employees' Facebook communications; the NLRB found firings for Facebook use by employees discussing complaints about their jobs. Design Tech. Grp., LLC, No. 20-CA-035511 (2017), 2017 WL 4925473 (N.L.R.B.), at *1.

Employers might want to view an employee's social media activities for several reasons. Employers may want to be sure that an employee is not disparaging the workplace, may want to monitor communications in order to comply with a statute or regulation,[185] or may want to exploit employees' social media accounts to advertise a business's products and service.[186] Nonetheless, a great deal of potential postings from individuals will fall well outside any of those legitimate areas of concern, and requiring tactful inattention to media activities in which the employer does not have a sufficient and legitimate interest protects the employee's privacy while still addressing an employer's legitimate concerns.

Currently, several states expressly prohibit employers from requiring applicants to provide personal passwords to employers.[187] In addition, a few states prohibit an employer from compelling an employee to access a personal online account in the employer's presence, that is, "shoulder surfing."[188] These

---

[185] *See, e.g.*, Fin. Indus. Regulatory Auth., *Social Media Web Sites: Guidance on Blogs and Social Networking Web Sites*, REG. NOTICE (Jan. 2010), http://www.finra.org/sites/default/files/NoticeDocument/p120779.pdf.

[186] See Joseph J. Lazzarotti, *Workplace Privacy, Data Management & Security Report: States Continue To Protect the Personal Social Media Accounts of Employees, with Oregon Likely to Add an Interesting Twist* (May 28, 2015), http://www.workplaceprivacyreport.com/2015/05/articles/workplace-privacy/states-continue-to-protect-the-personal-social-media-accounts-of-employees-with-oregon-likely-to-add-an-interesting-twist/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+WorkplacePrivacyDataManagementSecurityReport+%28Workplace+Privacy%2C+Data+Management+%26+Security+Report%29.

[187] ARK. CODE ANN. § 11-2-124 (West 2018); CAL. LAB. CODE § 980 (West 2018); COLO. REV. STAT. ANN. § 8-2-127 (West 2018) (password prohibition limited to access through the employee's or applicant's "personal electronic communication device"); CONN. GEN. STAT. ANN. § 31-40X (West 2018); DEL. CODE ANN. tit. 19, § 709A (West 2018); 820 ILL. COMP. STAT. ANN. 55/10 (West 2018); LA. STAT. ANN. §§ 51:1951–1955 (West 2018); ME. REV. STAT. ANN. tit. 26, §§ 616–619 (2017); MD. CODE ANN. LAB. & EMPL. § 3-712 (West 2018); MICH. COMP. LAWS ANN. § 37.278 (West 2018); NEB. REV. STAT. ANN. § 48-3503 (West 2018); NEV. REV. STAT. ANN. § 613.135 (West 2017); N.H. REV. STAT. ANN. § 275:74(II) (2018); N.J. STAT. ANN. §§ 34:6B-5–10 (West 2018); N.M. STAT. ANN. § 50-4-34 (West 2018); OKLA. STAT. ANN. tit. 40, §§ 173.2, 173.3 (West 2018); OR. REV. STAT. ANN. § 659A.330 (West 2018); 28 R.I. GEN. LAWS ANN. § 28-56-1-6 (West 2017); TENN. CODE ANN. §§ 50-1-1001–1004 (West 2018); UTAH CODE ANN. §§ 34-48-101–301 (West 2018); VIR. CODE ANN. § 40.1-28.7:5(B) (West 2018); WASH. REV. CODE ANN. §§ 49.44.200, 205 (West 2018); WIS. STAT. ANN. § 995.55 (West 2017).

[188] *See, e.g.*, OR. REV. STAT. ANN. § 659A.330(1)(c) (2015); TENN. CODE ANN. § 50-1-1003(a)(3) (2014); WASH. REV. CODE ANN. § 49.44.200(1)(b) (West 2013); WIS. STAT. ANN. § 995.55(2)(a)(1); *see also* Susan Park, *Employee Internet Privacy: A Proposed Act That Balances Legitimate Employer Rights and Employee Privacy,* 51 AM. BUS. L.J. 779, 790 (2014).

model tactful inattention by prohibiting employers from demanding "key" information that they know would provide them access to personal information about the employee.

In addition to prohibiting employers from asking an employee or applicant for a social media password, many of the statutes provide that employers who inadvertently receive an employee's login information may not use it to log into the employee's account.[189] This is an example of a statute requiring tactful inattention to information within one's reach.

Such laws reflect that given modern social media, information that individuals may have once shared over a phone or in a face-to-face conversation, hidden from the employer's gaze, may now appear on social media, where an employer may be able to access it, at least with the employee's credentials. But these laws help stem the pullback on privacy of these advances in communication, imposing on employers a duty to avoid peeping. The information may be available in the cybersphere, but that does not mean that employers have a right to access it, and if they do get their hands on the "key" to it, they may not exploit that power to access.

B. Use of Consumers' Online Information by Political Campaigns and Vendors

While employers may want to surveil their employees to keep them in check, political campaigns and vendors may want to obtain individuals' data to manipulate their votes and their purchases. The power and availability of such data calls for tactful inattention.

In 2015, Dr. Aleksandr Kogan, a professor at Cambridge University, sought data from Facebook for an app he created called "mydigitallife," which purported to be a personality assessment for use by psychologists.[190] Facebook claimed that

---

[189] *See, e.g.*, ARK. CODE ANN. § 11-2-124(b)(3); 820 ILL. COMP. STAT. ANN. 55/10(b)(4); LA. STAT. ANN. § 51:1953(C); NEB. REV. STAT. § 48-3510; N.H. REV. STAT. ANN. § 275:74(V); OKLA. STAT. ANN. tit. 40, § 173.2(C); OR. REV. STAT. ANN. § 659A.330(6); VIR. CODE ANN. §§ 40.1-28.5(C), 28.7(C) (West 2018); WASH. REV. CODE ANN. § 49.44.200(4); W. VA. CODE ANN. § 21-5H-1(c) (West 2018); WIS. STAT. ANN. § 995.55(7)(d).

[190] Nicole Banas, *Facebook Execs Liable for "Massive" Data Scandal, Investor Suit Says*, WESTLAW SECS. ENFORCEMENT & LITIG. DAILY BRIEFING, 2018 WL 1473644 (Mar. 27, 2018).

Dr. Kogan said he wanted the data for academic purposes.[191] But Dr. Kogan had been hired by Cambridge Analytica, a political consulting firm, the month the company was founded by Stephen Bannon[192] with Robert Mercer, a Republican party donor.[193] Mr. Bannon later became chief White House strategist to President Trump.[194] Dr. Kogan's app provided Cambridge Analytica access to 87 million Facebook users' data,[195] which it used to influence voters to support Trump's candidacy.[196] Under the secrecy paradigm, a data broker may use the data without restriction. In contrast, a tactful inattention approach might require those that possess social media users' search, "like," and posting information to refrain from using it in such ways.

Such an approach appears in a Congressional bill drafted in response to the Cambridge Analytica scandal by Senators Markey and Blumenthal.[197] Somewhat cumbersomely entitled the "Customer Online Notification for Stopping Edge-provider Network Transgressions Act" (the "CONSENT Act"), the bill would require data sellers, called "edge providers" in the bill,[198]

---

[191] Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[192] Matthew Rosenberg, *Professor Apologizes for Helping Cambridge Analytica Harvest Facebook Data*, N.Y. TIMES (Apr. 22, 2018), https://www.nytimes.com/2018/04/22/business/media/cambridge-analytica-aleksandr-kogan.html.

[193] William Booth & Karla Adam, *Cambridge Analytica's Alexander Nix: Bong Villain, Tech Genius, or Hustler?*, WASH. POST (Mar. 27, 2018), https://www.washingtonpost.com/world/europe/cambridge-analyticas-alexander-nix-bond-villain-tech-genius-or-hustler/2018/03/27/14c99112-2e34-11e8-8dc9-3b51e028b845_story.html?utm_term=.c672d64a3831.

[194] Jose A. DelReal, *Trump Draws Sharp Rebuke, Concerns over Newly Appointed Chief White House Strategist Stephen Bannon*, WASH. POST (Nov. 13, 2016), https://www.washingtonpost.com/news/post-politics/wp/2016/11/13/trump-draws-sharp-rebuke-concerns-over-newly-appointed-chief-white-house-strategist/?noredirect=on&utm_term=.9e145906f9a9.

[195] Sarah Emerson, *Mark Zuckerberg: "It Was My Mistake" Facebook Compromised Data of 87 Million Users*, MOTHERBOARD (Apr. 4, 2018, 5:44 PM), https://motherboard.vice.com/en_us/article/7xdw99/mark-zuckerberg-it-was-my-mistake-facebook-compromised-data-of-87-million-users.

[196] Rosenberg et al., *supra* note 191. The company created profiles based on individual features such as age, gender, ethnicity, race, income, advertising resonance, consumer and lifestyle data, and political engagement. Mark Andrus, *The New Oil: The Right To Control One's Identity in Light of the Commoditization of the Individual*, A.B.A. BUS. L. TODAY (Sept. 2017), https://www.americanbar.org/groups/business_law/publications/blt/2017/09/06_andrus.html.

[197] S. 2639, 115th Cong. (2017–2018).

[198] The bill defines "edge provider[s]" as those providing an "edge service," which is one provided over the Internet that meets any of four criteria, including one

to, among other requirements, "obtain opt-in consent from a customer to use, share, or sell the sensitive customer propriety information."[199] Furthermore, the bill would restrict a preferred dodge around such privacy provisions, whereby service providers simply deny the service to non-compliant customers; the bill would prohibit an edge provider from imposing "take-it-or-leave-it" conditions on the customer.[200] Thus, services like Facebook would have to gain customers' explicit permission to sell their information to third parties such as Dr. Kogan—a tactful inattention to the content of such information and its commercial value.

While the federal response is at present merely a bill, the state of California responded to the Cambridge Analytica scandal with an emphatic and powerful privacy law, the California Consumer Privacy Act of 2018.[201] Under it, certain businesses[202] must, upon request provide information about their general collection practices to consumers, including information about the categories and specific pieces of personal information[203] the business has collected.[204] Furthermore, consumers have the right to request businesses to delete any collected personal information.[205] Those businesses that sell consumers' personal information or disclose it for business purposes also must, upon request, disclose to the consumer what they collected and sold

---

"through which a customer divulges sensitive customer proprietary information." *Id.* § 2(a)(4), (5).

[199] The bill does not impose this requirement directly on edge providers; rather, the bill calls for the Federal Trade Commission to promulgate regulations that impose such a requirement. *Id.* § 2(b)(2)(A), (B)(iii).

[200] *Id.* § 2(b)(2)(A), (B)(vi).

[201] California Privacy Act of 2018, ch. 55, 2018 Cal. Legis. Serv. (West), as amended by 2018 Cal. Legis. Serv. ch. 735 (to be codified CAL. CIV. CODE §§ 1798.100–198) (adding title 1.81.5 to part 4 of division 3 of the Civil Code). The Act becomes effective January 1, 2020. *Id.* § 3 (to be codified at CAL. CIV. CODE § 1798.198(a)). The Act refers explicitly to the Cambridge Analytica revelations. *Id.* § 2(g).

[202] The Act defines "business[es]" to mean designated organizations "operated for profit or financial benefit . . . that collect[] consumers' personal information" and that meet one of three specified thresholds. *Id.* § 3 (to be codified at CAL. CIV. CODE § 1798.140(c)).

[203] This term is defined quite broadly to include identifiers, biometric information, and "Internet or other electronic activity information," among other items. *Id.* (to be codified at CAL. CIV. CODE § 1798.140(o)). However, the term excludes "publicly available information." *Id.* (to be codified at CAL. CIV. CODE § 1798.140(o)(2)).

[204] *Id.* (to be codified at CAL. CIV. CODE §§ 1798.100, 1798.110).

[205] *Id.* (to be codified at CAL. CIV. CODE § 1798.105(a)).

about that consumer.[206] As a key matter, consumers can opt-out of the sale by a business of their personal information,[207] and businesses may not discriminate against consumers who exercise their rights, although a business may charge different prices or provide different levels of quality if the "difference is reasonably related to the value provided to the consumer by the consumer's data," a potentially enormous loophole.[208] Nonetheless, California's Consumer Privacy Act represents a potent tactful inattention approach to maintaining the privacy of individual's digital data.

While political campaigns may seek a consumer's individual information to amass power, vendors and advertisers seek it to create a picture of a consumer's personality to market goods and services, tailor responses,[209] and even create "boutique" pricing, individually targeted to leverage the most money out of any given consumer.[210] Relatedly, the burgeoning field of "neuromarketing" seeks to study brain activity in response to stimuli to understand consumer preferences.[211] Advertisers increasingly make secondary use of information that they think gives cues as to an individual's personality to shape advertising and target that individual in a manner that the advertisers think will be specifically appealing.[212] Such personality profiling may not always necessarily hurt a given consumer, but laws in the mode of tactful inattention could help skew such uses to the consumer's benefit and away from the consumer's detriment.

---

[206] *Id.* (to be codified at CAL. CIV. CODE § 1798.115(a)).

[207] *Id.* (to be codified at CAL. CIV. CODE § 1798.120(a)).

[208] *Id.* (to be codified at CAL. CIV. CODE § 1798.125(a)(1), (2)). The bill specifically lists the denial of goods or services, the charging of different prices, and the providing of different levels of goods or services among the prohibited acts of discrimination. *Id.* (to be codified at CAL. CIV. CODE § 1798.125(a)(A)–(C)). However, businesses may offer financial incentives. *Id.* (to be codified at CAL. CIV. CODE § 1798.125(b)).

[209] *See infra* text accompanying notes 213–14.

[210] *See infra* text accompanying note 216.

[211] *See* Sandra Blakeslee, *If Your Brain Has a "Buy Button," What Pushes It?*, N.Y. TIMES (Oct. 19, 2004), https://nytimes.com/2004/10/19/science/if-your-brain-has-a-buybutton-what-pushes-it.html; G. A. Calvert & M. J. Brammer, *Predicting Consumer Behavior: Using Novel Mind-Reading Approaches*, PubMed ID 22678839 (describing advances in medical learning to help improve "greater accuracy of prediction in terms of consumer acceptance of new brands, products, and campaigns").

[212] *See, e.g.*, Joanna Penn, *Behavioral Advertising: The Cryptic Hunter and Gatherer of the Internet*, 64 FED. COMM. L.J. 599, 601 (2012).

For instance, an advertiser could use consumer-specific purchasing patterns to target a particular consumer and manipulate him or her into behavior more favorable to a particular merchant. A scenario sketched by Professor Tal Z. Zarsky illustrates the kind of manipulation that a savvy seller could engage in, one who notices that a consumer has stopped buying cigarettes and has bought a nicotine patch.[213] Deducing that the consumer seeks to cease smoking, the merchant could target him with cigarette ads and even free cigarettes.[214]

Vendors could also use such data to analyze consumer behavior in the marketplace, tailoring their own behavior towards a particular consumer. For instance, radio frequency identification tags could help identify "undesirable customers" who "monopolize the attention of attendants" before leaving without buying.[215] What are some other practical uses of these indicators of personality traits that our purchasing, surfing, and postings may give away? As Professor Lior Jacob Strahilevitz discusses, merchants and service providers could use consumer data to discriminate among customers on the basis of their wealth in providing them services, so information privacy could benefit poor consumers by "thwarting" such sorting.[216]

One lucrative use of information about personal preferences is to engage in "weblining"—charging higher prices to certain consumers based on the preferences revealed by their online activity.[217] According to one study, such practices, known by economists as "first-degree price discrimination," but commonly

---

[213] Tal Z. Zarsky, *"Mine Your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion*, 5 YALE J.L. & TECH. 4, 20 (2002–2003).

[214] *Id.*

[215] Jonathon Zittrain, *Privacy 2.0*, U. CHI. LEGAL F. 65, 72 (2008).

[216] Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2029 (2013) ("Protecting privacy seems to thwart price and service discrimination while fostering statistical discrimination on the basis of race and gender and lowering production costs."). He speculates on the implications for the use of big data and the political process, given that it appears that introverts are less likely to participate in the process. *Id.* at 2025.

[217] *See, e.g.*, Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 SEATTLE U. L. REV. 439, 450–51 (2011); Zittrain, *supra* note 215, at 72 (describing how information about individual behavior can help enable price discrimination). Some have defended the ability of firms to engage in this kind of price discrimination as possibly benefiting consumers and the market alike. *See* Matthew A. Edwards, *Price and Prejudice: The Case Against Consumer Equality in the Information Age*, 10 LEWIS & CLARK L. REV. 559, 559 (2006).

as "dynamic pricing," are increasing.[218] By using detailed personal profiles of shoppers pulled from tracked data, retailers can "apply sophisticated pricing models to individual consumer profiles through automated price-setting systems in order to target personalized prices to individual consumers."[219]

Pricing discrimination is not a new concept. Some states prohibit price discrimination under certain circumstances, usually in the context of a competitor's discrimination intended to hinder competition.[220] In addition, § 2(a) of the federal Robinson-Patman Act prohibits certain kinds of price discrimination, but without any right to a private cause of action.[221] But the Robinson-Patman Act has not been used to

---

[218] JOSEPH TUROW ET AL., OPEN TO EXPLOITATION: AMERICAN SHOPPERS ONLINE AND OFFLINE 10 (Annenberg Pub. Pol'y Ctr. of Univ. of Pa. ed., 2005), http://www.annenbergpublicpolicycenter.org/wp-content/uploads/Turow_APPC_Report_WEB_FINAL2.pdf.

[219] Akiva A. Miller, *What Do We Worry About When We Worry About Price Discrimination? The Law and Ethics of Using Personal Information for Pricing*, 19 J. TECH. L. & POL'Y 41, 49–50 (2014). The author notes that data brokers offer a variety of options to retailers to reach not just their own prior shoppers, but shoppers of competitors as well. *Id.* at 52.

[220] *See, e.g.*, COLO. REV. STAT. ANN. § 3 6-2-103(1) (West 2018); Dunlap v. Colo. Springs Cablevision, Inc., 829 P.2d 1286, 1296 (Colo. 1992) (en banc) (plaintiffs, consumers, could sue to enforce state anti-price discrimination provision even though scope is limited "to conduct intended to destroy or prevent primary-line competition"). *But see* Perdue v. Crocker Nat'l Bank, 38 Cal. 3d 913, 930 (1985) (affirming demurrer of deceptive trade practices act claim based on bank's " 'arbitrary' price discrimination" of waiving NSF charges for some customers but not others, reasoning that such a waiver did not "describe[] acts of unfair competition").

[221] Robinson-Patman Act, 15 U.S.C. § 13(a) (2012). The provision states as follows:

> It shall be unlawful for any person engaged in commerce, in the course of such commerce, either directly or indirectly, to discriminate in price between different purchasers of commodities of like grade and quality, where either or any of the purchases involved in such discrimination are in commerce, where such commodities are sold for use, consumption, or resale within the United States or any Territory thereof or the District of Columbia or any insular possession or other place under the jurisdiction of the United States, and where the effect of such discrimination may be substantially to lessen competition or tend to create a monopoly in any line of commerce, or to injure, destroy, or prevent competition with any person who either grants or knowingly receives the benefit of such discrimination, or with customers of either of them.

Id. See also Douglas M. Kochelek, Note, *Data Mining and Antitrust*, 22 HARV. J. L. & TECH. 515, 523–24 (2009) (also discussing the Sherman Act's applicability to price discrimination).

The Federal Trade Commission has sued sellers who have sold products to different customers at "discriminatory" prices, although these cases also seem to be directed to actions intended to hamper competition, as opposed to maximize profits.

prohibit modern "weblining" or "boutique pricing" at the consumer level or in the context of the new data that can powerfully target individuals. As an example, Zarsky writes about the hypothetical situation of a wealthy philosophy student whose book buying behavior leads an online retailer to charge him more, generally, and even more during the times the seller has determined the student is most likely to want books.[222]

This sort of use of consumer-specific information can provoke outrage—even in Internet-savvy consumers. Professor William W. Fisher writes that consumers often respond strongly and negatively to such practices.[223] Fisher cites Amazon.com's experiment with "dynamic pricing," whereby it was believed that Amazon quoted higher prices to existing Amazon customers than to new ones.[224] In part, Fisher writes, the anger arose from the surreptitious use of the practice believed to have taken place.[225] Another study of consumer reactions to "dynamic pricing" found that between 87%–91% of the consumers surveyed disagreed with statements along the lines of "It [i]s OK if [a supermarket or online store] charges different people different prices for the same products during the same hour."[226]

Aside from the unfairness perception that Professor Fisher discusses, Professor Zarsky identifies a particular concern about such surreptitious use of data to profile consumers, whether to create a personal price or to market a particular product: it can be inaccurate, leading to unjust treatment of a consumer.[227] In

See, e.g., FTC v. Hunt Foods & Indus., Inc., 178 F. Supp. 448, 454 (S.D. Cal. 1959), *aff'd*, 286 F.2d 803 (9th Cir. 1960). Furthermore, some case law approves of price changing so long as the seller charges all competing customers the same amount at any given time, indicating that contemporaneous price discrimination would be unlawful. *See, e.g.*, K-S Pharm., Inc. v. Am. Home Prods. Corp., 962 F.2d 728, 733 (7th Cir. 1992); A.A. Poultry Farms, Inc. v. Rose Acre Farms, Inc., 881 F.2d 1396, 1406-08 (7th Cir. 1989); Tex. Gulf Sulphur Co. v. J.R. Simplot Co., 418 F.2d 793, 806 (9th Cir. 1969); Xi v. Apple, Inc., 603 F. Supp. 2d 464, 468 (E.D.N.Y. 2009). The Illinois Supreme Court concluded that an insurance company's failure to disclose to home buyers that it had paid rebates to institutions that had bought the insurance on the home buyers' behalf, thus reducing the actual cost of the insurance but without benefitting the buyers, could be an actionable deceptive trade practice under state law. Fitzgerald v. Chi. Title & Trust Co., 380 N.E.2d 790, 794–95 (Ill. 1978).

[222] Zarsky, *supra* note 213, at 19.

[223] William W. Fisher, III, *When Should We Permit Differential Pricing of Information?*, 55 UCLA L. REV. 1, 10 (2007) (describing the perception of consumers to such practices as "gouging").

[224] *Id.* at 11–12.

[225] *Id.* at 12.

[226] TUROW ET AL., *supra* note 218, at 22.

[227] Zarsky, *supra* note 213, at 47–50.

his hypothetical, a consumer could be charged a higher insurance premium simply because a consumer was erroneously classified as high-risk.[228] In another hypothetical, an insurer wrongly classifies an insured as someone who enjoys high risk sports, inferred from her reading and web browsing activity, and accordingly raises her insurance premium, even though in fact the consumer leads a conservative life and has made her choices for an article she's writing, not to enhance her own leisure activities.[229] Such surreptitious labeling can be completely invisible to us, and as impossible to fix as it is to detect.

From a tactful inattention standpoint, legislators could regulate the use of individual data for personality profiling, whether used for marketing, service tailoring, or price targeting. Thus, the mere fact that troves of individually identifiable consumer data were available, were no longer "secret," would not mean that the data was fair game for simply any use a data miner could dream up. Rather, legislators could accede to the wishes of individuals about how they want their data used, changing the balance of power between merchants and their targets.

IV. BENEFITS OF THE TACTFUL INATTENTION PARADIGM IN LAW

Laws adopting a tactful inattention paradigm shift the balance of power and thereby change the intensity of scrutiny: if we move the burden of protecting information toward those who want to exploit others' data, they might put less energy into inquisitiveness, into voyeurism. If we reduce or eliminate the profit to which disinterred information can be devoted, then

---

[228] *Id.* at 49.

[229] *Id.* at 21. Zarsky examines the likely consequences of price discrimination techniques like this one, along with the likelihood of prohibited profiling techniques that the practice of "Weblining" can produce. *Id.* at 25–26, 47–50. He notes as well the information imbalance that arises to the consumer's detriment when the seller has a lot of information about the customer's "demand curve" and "reserve price," and the consumer's ignorance of corresponding information on the other side. *Id.* at 30–31. "The practical consequences of this phenomenon are poor and misinformed people paying higher prices for products due to ignorance of information market dynamics." *Id.* at 31. *See also* Nathan Newman, *The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google*, 40 WM. MITCHELL L. REV. 849, 852–53 (2014) (discussing possible consequences of Google's mechanism that allows advertisers to target specific users, such as payday lenders and subprime mortgage lenders, to find financially imperiled consumers). Concerned with "online behavioral targeting" on the basis of race, Professor Newman argues for "a detailed and explicit 'opt-in' consent" for Google to collect certain data. *Id.* at 886.

others will be less motivated to unearth the personal and sensitive information to begin with. By moving away from the secrecy paradigm towards the tactful inattention paradigm, we can help promote advantageous uses of personally identifiable information such as those for medical research.[230] For example, large aggregate patient databases are being mined for research due to their rich nature. [231] The secrecy paradigm may rely on the anonymization of data—treating as "secret" information that has supposedly been peeled of individual markers—"deidentified," in HIPAA's parlance[232]—but modern technology continues to defeat anonymizing techniques.[233] Alternatively, forced anonymization of data can strip the usefulness of data for researchers.[234] By recognizing that such data may be personally identifiable—that is, it may have lost its secrecy—but forbidding certain uses of it, we can preserve the usefulness of the data to medical research while still preventing its original sources from being unduly harmed by its "visibility."

By prohibiting specific uses of information, a tactful inattention-focused law can guard against a harm Professor Solove identifies: "[t]he risk of disclosure [that] can prevent people from engaging in activities that further their own self-development."[235] The tactful inattention paradigm can also address the law's tendency to permit disclosure that would otherwise be prohibited but for the fact that others know of it.[236]

This is not to argue that the secrecy paradigm is useless and should be replaced wholesale. Tactful inattention cannot satisfactorily resolve all injuries to privacy. Some injuries result from the sheer and simple exposure of certain information itself.

---

[230] *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1866–68 (2011) (describing the benefits of data for medical research).

[231] Marc A. Rodwin, *Patient Data: Property, Privacy & the Public Interest*, 36 AM. J. L. & MED. 586, 595–97 (2010).

[232] 45 C.F.R. § 164.514(a). *See also supra* text accompanying notes 87–93.

[233] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1705 (2010) (describing the problems of "reidentification" of data).

[234] *Id.* at 1714. With respect to the anonymizing of health data, technology has been developing the reconstruction of facial and cranial features from brain images that might make reidentification of those images a possibility. *See* Judy Illes & Sofia Lombera, *Identifiable Neuro Ethics Challenges to the Banking of Neuro Data*, 10 MINN. J. L. SCI. & TECH. 71, 79 (2009).

[235] *See* Solove, *A Taxonomy of Privacy*, *supra* note 119, at 529–30.

[236] *Id.* at 531 ("The law often protects against disclosure when the information is kept secret but not when others know about it.").

Professor Solove specifically identifies "deeply primordial" information that "is not revealing of anything we typically use to judge people's character."[237] The secrecy paradigm, enforced through social conventions, remains necessary for this type of information.

Rather, it is to urge the consideration of a different, potentially supplementary approach in certain contexts. Neither paradigm serves well in all instances. Professor Jerry Kang, in writing about information privacy in cyberspace and surveillance,[238] discusses the problem of general laws governing the flow of all personal information that would "constrain too often even casual observation."[239] He was writing of the difference between regulating the flow of personal information in real space as opposed to cyberspace,[240] but the same issues can arise in cyberspace with digital information.

Furthermore, while technology has heightened the availability of personal data, it may also help implement the tactful inattention paradigm. For instance, Professor Paul Ohm has compared attempts to keep personally identifiable information from being reidentified to the game of "whack-a-mole."[241] However, by working with technology to identify tracking and auditing functions to control the use, rather than the observation, of data, we can work *with* developing technology instead of *against* it, and we can monitor and identify uses of personal data. Professor Ohm argues that computer security research can lead to techniques to monitor access controls and audit trails, permitting users to interact with the data only in predetermined, limited ways, and recording users' use of data.[242] In this way, laws modeled on the tactful inattention paradigm can be enforced, calling out users' uses, rather than targets' slips.

In summary, the tactful inattention paradigm offers an alternative, or perhaps supplementary approach, to protecting privacy that can be an effective option in some circumstances, while not serving the best balance of interests in others.

---

[237] *Id.* at 533.

[238] *See* Jerry Kang, I*nformation Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1988).

[239] *Id.* at 1268.

[240] *Id.*

[241] Ohm, *supra* note 233, at 1742.

[242] *Id.* at 1757.

CONCLUSION

The secrecy paradigm may have served the analog age profitably well, but sensitive data is simply too accessible for that paradigm to continue as the model for all privacy laws. The nature of information and people's relationship to it has changed, but people continue to need privacy to flourish as individuals and in our relationships.

Erving Goffman's tactful inattention concept can serve as the basis of a new paradigm, one that requires us to avert our eyes from data when using it would unjustifiably impair someone's privacy. Aspects of American law have long used such a paradigm, such as in evidence law and Peeping Tom statutes. Recently, legislatures have been turning to a tactful inattention model for legislation addressing some of our modern information capabilities, such as in the GINA and the FCRA. Two areas ripe for continued implementation of the paradigm are employment law and the use by employers of their employees' social media information, and the use by political campaigns and vendors of the data consumers cannot help but leave behind in their forays on the Internet. A tactful inattention paradigm, by recognizing that digital data has become widely accessible, can redistribute the responsibility for preventing sensitive information's misuse and thereby reinvigorate privacy law to promote human flourishing.